Defense Department
Intelligence and Security
Doctrine, Directives and Instructions

Doctrine is the fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (Joint Pub 1-02)

The joint publication hierarchy provides a framework for joint doctrine and joint tactics, techniques, and procedures. The organizational structure follows traditional joint staff lines of responsibility to the maximum degree possible. Each series provides for a keystone manual as the first publication in the series. The keystone manuals constitute the doctrinal foundation of the series. There are a number of online sources for joint doctrine and related publications.

The Department of Defense (DoD) issues a large number of Directives and Instructions. The purpose of these issuances varies; however, all of them are used to internally manage the business of the DoD.

DoD Directives are broad DoD policy documents containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by the DoD Components within their specific areas of responsibilities. DoD Directives establish or describe policy, programs, and organizations; define missions; provide authority; and assign responsibilities.

DoD Instructions implement the policy, or prescribes the manner or a specific plan or action for carrying out the policy, operating a program or activity, and assigning responsibilities.

The DoD Directives and Instructions are numbered according to the following eight major subject groups:

- 1000 - Manpower and Personnel (Civilian, Military, and Reserve)
- 2000 - International and Foreign Affairs
- 3000 - Plans and Operations, Research and Development, Intelligence, and Computer Language
- 4000 - Logistics, Natural Resources, and Environment
- 5000 - Acquisition and Administrative Management, Organizational Charters, Security, and Public and Legislative Affairs
- 6000 - Health
- 7000 - Budget, Finance, Audits, and Information Control
- 8000 - Information Management

JCS Joint Publications

- United States Government Glossary of Interagency and Associated Terms, July 2017
- JP 1, Doctrine for the Armed Forces of the United States 25 March 2013, Incorporating Change 1, 12 July 2017
- JP 1-0, Joint Personnel Support 01 December 2020
- Department of Defense Dictionary of Military and Associated Terms as of November 2021
- JP 1-05, Religious Affairs in Joint Operations 20 November 2013
- JP 2-0, Joint Intelligence, 22 October 2013
  - JP 2-01, Joint and National Intelligence Support to Military Operations, 5 July 2017

    - JP 2-01.1, Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting, 9 January 2003
    - JP 2-01.2, Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations
    - JP 2-01.3, Joint Intelligence Preparation of the Operational Environment, 21 May 2014
    - JP 2-02, National Intelligence Support to Joint Operations, 28 September 1998
    - JP 2-03, Geospatial Intelligence in Joint Operations , 5 July 2017
- JP 3-0, Joint Operations, 17 January 2017, Incorporating Change 1, 22 October 2018
- JP 3-01, Countering Air and Missile Threats, 21 April 2017
- JP 3-01.1, Aerospace Defense of North America, 4 November 1996
- JP 3-02, Amphibious Operations, 4 January 2019
- JP 3-03, Joint Interdiction, 9 September 2016
- JP 3-04, Joint Shipboard Helicopter and Tiltrotor Aircraft Operations, 06 December 2012
- JP 3-05. Special Operations, 16 July 2014
- JP 3-06. Joint Urban Operations, 20 November 2013
- JP 3-07. Stability, 03 August 2016
- JP 3-07.2, Joint Tactics, Techniques, and Procedures for Antiterrorism, 17 March 1998
    - APPENDIX J THREATCON SYSTEM
- JP 3-07.3, Peace Operations, 01 March 2018 (via Public Intelligence)
- JP 3-07.4, Counterdrug Operations, 5 February 2019
- JP 3-08, Interorganizational Cooperation, 12 October 2016
- JP 3-09, Joint Fire Support, 10 April 2019
- JP 3-09.3, Close Air Support, 25 November 2014
- JP 3-10, Joint Security Operations in Theater, 25 July 2019
- JP 3-11, Operations in Chemical, Biological, Radiological, and Nuclear Environments, 29 October 2018
- JP 3-12, Cyberspace Operations, 8 June 2018
- JP 3-13, Information Operations, 27 November 2012, incorporating Change 1, 20 November 2014
- JP 3-13.1, Electronic Warfare, 08 February 2012
- JP 3-13.2, Psychological Operations, 7 January 2010
- JP 3-13.3, Operations Security, 06 January 2016 (via Public Intelligence)
- JP 3-13.4, Military Deception, 14 February 2017 (2012 edition)
- JP 3-14, Space Operations, 10 April 2018, with change 1, 26 October 2020
- JP 3-15, Barriers, Obstacles, and Mine Warfare for Joint Operations, 06 September 2016
- JP 3-15.1, Counter-Improvised Explosive Device Operations, 09 January 2012
- JP 3-16, Multinational Operations, 01 March 2019
- JP 3-17, Air Mobility Operations, 5 February 2019
- JP 3-18, Joint Forcible Entry Operations, 11 May 2017, Incorporating Change 1 9 January 2018
- JP 3-20, Security Cooperation, 23 May 2017
- JP 3-22, Foreign Internal Defense, 17 August 2018
- JP 3-24, Counterinsurgency, 25 April 2018
- JP 3-25, Countering Threat Networks, 21 December 2016
- JP 3-26, Counterterrorism 24 October 2014
- JP 3-27, Homeland Defense 10 April 2018
- JP 3-28, Defense Support of Civil Authorities 29 October 2018
- JP 3-29, Foreign Humanitarian Assistance 14 May 2019
- JP 3-30, Joint Air Operations 25 July 2019
- JP 3-31, Joint Land Operations, 03 October 2019
- JP 3-32, Joint Maritime Operations, 8 June 2018, Incorporating Change 1, 20 September 2021
- JP 3-33, Joint Task Force Headquarters, 30 July 2012
- JP 3-34, Joint Engineer Operations, 06 January 2016
- JP 3-35, Deployment and Redeployment Operations, 10 January 2018
- JP 3-40, Joint Countering Weapons of Mass Destruction, 27 November 2019
- JP 3-41, Chemical, Biological, Radiological, and Nuclear Response, 09 September 2016
- JP 3-50, Personnel Recovery, 20 December 2011
- JP 3-51, Joint Doctrine for Electronic Warfare, 7 April 2000
- JP 3-52, Joint Airspace Control, 13 November 2014
- JP 3-53, Doctrine for Joint Psychological Operations, 5 September 2003
- Joint Pub No. 3-55 - Reconnaissance, Surveillance, and Target Acq Sppt for Joint Op April 14, 1993
- Joint Pub No. 3-55.1 - JTTP for Unmanned Aerial Vehicles 27 August 1993
- Joint Pub No. 3-56.1 - Command and Control for Joint Air Operations 14 Nov 1994
- JP 3-57, Civil-Military Operations, 9 July 2018
- JP 3-59, Meteorological and Oceanographic Operations, 10 January 2018
- JP 3-60, Joint Targeting, 31 January 2013

- JP 3-61, Public Affairs 17 November 2015, Incorporating Change 1, 19 August 2016
- JP 3-63, Detainee Operations, 13 November 2014
- JP 3-68, Noncombatant Evacuation Operations, 18 November 2015
- JP 3-72, Joint Nuclear Operations, 17 April 2020 (2019 edition)
- JP 3-80, Resource Management, 11 January 2016
- JP 3-84, Legal Support, 02 August 2016
- JP 3-85, Joint Electromagnetic Spectrum Operations, 22 May 2020
- JP 4-0, Joint Logistics 4 February 2019, Incorporating Change 1, 8 May 2019
- JP 4-01, The Defense Transportation System 18 July 2017
- JP 4-02, Joint Health Services 17 December 2017, incorporating Change 1, 28 September 2018
- JP 4-03, Joint Bulk Petroleum and Water Doctrine 11 January 2016
- JP 4-04, Contingency Basing 4 January 2019
- JP 4-05, Joint Mobilization Planning 23 October 2018
- JP 4-06, Mortuary Affairs 12 October 2011
- JP 4-08, Logistics in Support of Multinational Operations 5 July 2017
- JP 4-09, Distribution Operations 05 February 2010
- JP 4-10, Operational Contract Support 04 March 2019
- JP 5-0, Joint Planning, 01 December 2020
- JP 6-0, Joint Communications System 10 June 2015, Incorporating Change 1, 04 October 2019
- JP 6-01, Joint Electromagnetic Spectrum Management Operations 20 March 2012

Military Tribunals

Regulation for Trial by Military Commission (2011 Edition), November 2011

Manual for Military Commissions (2010 Edition), April 2010

Military Commission Instructions

- Instruction No. 1: Guidance on Military Commission Instructions themselves
- Instruction No. 2: Crimes and Elements for Trials by Military Commission
- Instruction No. 3: Responsibilities of the Chief Prosecutor, Prosecutors, and Assistant Prosecutors
- Instruction No. 4: Responsibilities of the Chief Defense Counsel, Detailed Defense Counsel, and Civilian Defense Counsel
- Instruction No. 5: Qualification of Civilian Defense Counsel
- Instruction No. 6: Reporting Relationships for Military Commission Personnel
- Instruction No. 7: Sentencing
- Instruction No. 8: Administrative Procedures
- Instruction No. 9: Review of Military Commission Proceedings

- Military Commission Instruction (draft), February 28, 2003

Military Commission Orders

- Order No. 1: Procedures for Trials by Military Commissions of Certain Non-United States Citizens in the War Against Terrorism
- Order No. 2: Designation of Deputy Secretary of Defense as Appointing Authority
- Order No. 3: Special Administrative Measures for Certain Communications Subject to Monitoring
- Order No. 4: Designation of Deputy Appointing Authority
- Order No. 5: Designation of Appointing Authority

Joint Chiefs of Staff Policy Documents

- Joint Strategy for Biological Warfare Defense, Chairman of the Joint Chiefs of Staff Instruction 3112.01B, 2 November 2012
- Defense Response to Chemical, Biological, Radiological, and Nuclear (CBRN) Incidents in the Homeland, Chairman of the Joint Chiefs of Staff Instruction CJCSI 3125.01D, 07 May 2015
- Military Support to Foreign Consequence Management Operations for Chemical, Biological, Radiological, and Nuclear Incidents, Chairman of the Joint Chiefs of Staff Instruction 3214.01E, 28 May 2015
- Program for Detainee Operations, Chairman of the Joint Chiefs of Staff Instruction 3290.01B, 1 June 2012, Change 1, 17 February 2015

- Joint Military Intelligence Requirements Certification, Chairman of the Joint Chiefs of Staff Instruction 3312.01A, 23 February 2007
- Target Development Standards, Chairman of the Joint Chiefs of Staff Instruction 3370.01B, 6 May 2016
- Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations, Chairman of the Joint Chiefs of Staff Instruction 5221.01D, 1 May 2013
- Standardization of Military and Associated Terminology, Chairman of the Joint Chiefs of Staff Instruction 5705.01F, 01 May 2017
- Information Assurance (IA) and Support to Computer Network Defense (CND), Chairman of the Joint Chiefs of Staff Instruction 6510.01F, 09 February 2011
- Code Word, Nickname and Exercise Term Report, Chairman of the Joint Chiefs of Staff Manual 3150.29A, 23 April 1998
- Preservation of Historical Records of Operations Enduring Freedom and Noble Eagle and Pertaining to Iraq, Chairman of the Joint Chiefs of Staff Notice 5760, 7 September 2006, current as of 31 January 2008
- Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, rev. 2, 31 March 2001 [MS Word]

DOD Directives

- DODD 1300.22 Mortuary Affairs Policy, October 30, 2015, Incorporating Change 1, December 8, 2017
- DODD 1300.30 DoD Support of State, Official, Special Military, and First lady Funerals, August 24, 2021, Incorporating Change 1, February 16, 2023
- DODD 1322.18 Military Training, January 13, 2009, Incorporating Change 1, Effective February 23, 2017
- DODD 1344.10 Political Activities by Members of the Armed Forces, February 19, 2008
- DODD 1400.16 Inter-departmental Civilian Personnel Administration Support, October 30, 1970
- DODD 1400.34 DoD Civilian Intelligence Personnel Management System (CIPMS) November 16, 1994
- DODD 1400.35 Defense Civilian Intelligence Personnel System (DCIPS) September 24, 2007, incorporating change 1, September 1, 2009
- DODD 1442.11 Political Activity Rules for DoD Political Appointees, November 8, 2021

- DODD 2000.12 DoD Antiterrorism (AT) Program, August 18, 2003, current as of December 13, 2007
- DODD 2000.13 Civil Affairs, March 11, 2014, Incorporating Change 1, May 15, 2017
- DODD 2005.02E Maritime Domain Awareness (MDA) in the Department of Defense, March 31, 2015, Incorporating Change 1, May 12, 2017
- DODD 2060.01 Implementation of, and Compliance with, Arms Control Agreements, June 23, 2020
- DODD 2060.02 DoD Countering Weapons of Mass Destruction (WMD) Policy, January 27, 2017
- DODD S-2060.04 DoD Support to the National Technical Nuclear Forensics (NTNF) Program (U), April 1, 2009
- DODD 2167A, "Defense System Software Development."
- DODD 2310.01E DoD Detainee Program, March 15, 2022
- DODD 2310.07 Past Conflict Personnel Accounting Policy, April 12, 2017, Incorporating Change 1, April 23, 2018
- DoDD 2311.01 DoD Law of War Program, July 2, 2020

- DoDD 3000.03E DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy, April 25, 2013, Incorporating Change 1, September 27, 2017
- DoDD 3000.05 Stabilization, 13 December 2018
- DoDD 3000.06 Combat Support Agencies (CSAs), June 27, 2013, Incorporating Change 1, Effective July 8, 2016
- DoDD 3000.07 Irregular Warfare (IW), 28 August 2014, Incorporating Change 1, May 12, 2017
- DoDD 3000.09 Autonomy in Weapon Systems, January 25, 2023
- DoDD 3000.10 Contingency Basing Outside the United States, August 27, 2021
- DoDD 3002.01 Personnel Recovery in the Department of Defense, 16 April 2009, Incorporating Change 2, May 24, 2017
- DoDD 3020.04 Order of Succession Pursuant to Executive Order 13533 and the Federal Vacancies Reform Act of 1998, August 25, 2010
- DoDD 3020.40 Mission Assurance (MA), November 29, 2016, Change 1, effective September 11, 2018
- DoDD 3020.44 Defense Crisis Management, 4 June 2007, Incorporating Change 2, Effective August 22, 2019
- DoD Manual 3025.01, Volume 1 Defense Support of Civil Authorities: Overview, August 11, 2016, including Change 1, April 13, 2017
- DoD Manual 3025.01, Volume 2 Defense Support of Civil Authorities: Incident Response, August 11, 2016, including Change 1, April 12, 2017
- DoD Manual 3025.01, Volume 3 Defense Support of Civil Authorities: Pre-Planned DoD Support of Law Enforcement Agencies, Special Events, Community Engagement, and Other Non-DoD Entities, August 11, 2016,

including Change 1, April 13, 2017
- DoDD 3025.13 Employment of DoD Capabilities in Support of the U.S. Secret Service (USSS), Department of Homeland Security (DHS), October 8, 2010
- DoDD 3025.14 Evacuation of U.S. Citizens and Designated Aliens from Threatened Areas Abroad, February 26, 2013, Incorporating Change 1, November 30, 2017
- DoDD 3025.18 Defense Support of Civil Authorities (DSCA), December 29, 2010, Incorporating Change 2, Effective March 19, 2018
- DoDD 3100.10 Space Policy, August 30, 2022, Change 1, October 15, 2024
- DoDD 3115.09 DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, October 11, 2012, Incorporating Change 3 Effective October 29, 2020
- DoDD 3115.13 DoD Support to the High-Value Detainee Interrogation Group (HIG), December 9, 2010, Incorporating Change 3, August 26, 2020
- DoDD 3115.16 The Defense Warning Network, December 5, 2013, Incorporating Change 2, August 10, 2020
- DoDD 3115.18 DoD Access to and Use of Publicly Available Information (PAI), June 11, 2019, Incorporating Change 1, August 20, 2020
- DODD 3150.06 U.S. Nuclear Command and Control System Support Staff (NSS), May 24, 2013
- DODD 3150.08 DoD Response to U.S. Nuclear Weapon and Radiological Material Incidents, 27 November 2020
- DODD 3150.5 DoD Response to Improvised Nuclear Device (IND) Incidents, 24 March 1987
- DODD 3160.01 Homeland Defense Activities Conducted by the National Guard, 25 August 2008, Incorporating Change 2, June 6, 2017
- DODD 3222.04 Electronic Warfare (EW) Policy, March 26, 2014, Incorporating Change 1, Effective May 10, 2017
- DODD 3300.03 DoD Document and Media Exploitation (DOMEX), January 11, 2011, Incorporating Change 2, Effective November 2, 2020
- DODD 3305.5: General Defense Intelligence Program (GDIP) Management, May 9, 1986
- DODD 3310.1 International Intelligence Agreements
- DODD 3325.1 Foreign Materiel Program [SECRET] 18 September 1986
- DODD S-3325.02 Transfer of National Intelligence Collection Tasking Authority (NICTA), March 16, 2009
- DODD 3600.01, Information Operations (IO), May 2, 2013
- DODD 3610.01, Electromagnetic Spectrum Enterprise Policy, September 4, 2020
- DODD 3700.01, DoD Command and Control Enabling Capabilities, October 22, 2014, Incorporating Change 2, April 28, 2022
- DODD 3801.02, North Atlantic Treaty Organization (NATO) Special Operations Headquarters (NSHQ), May 28, 2019

- DODD 4180.01 DoD Energy Policy, April 16, 2014
- DODD 4500.54E DoD Foreign Clearance Program (FCP), May 31, 2022
- DODD 4630.5 Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems, November 12, 1992
- DODD 4640.6 Communications Security Telephone Monitoring and Recording, June 26, 1981
- DODD 4650.1 Policy for Management and Use of the Electromagnetic Spectrum, June 8, 2004
- DODD 4650.05 Positioning, Navigation, and Timing (PNT), June 9, 2016, Incorporating Change 2, April 8, 2021
- DODD 4715.21 Climate Change Adaptation and Resilience, January 14, 2016, Incorporating Change 2, January 16, 2025

- DODD 5000.01 The Defense Acquisition System, September 9, 2020, with Change 1, effective July 28, 2022
- DODD 5010.10 Intelligence Career Development Program, August 9, 1972
- DOD 5010.38 Management Control (MC) Program, August 26, 1996
- DODD 5025.1 Department of Defense Directives System, 27 July 2000
- DOD 5030.19 DoD Responsibilities on Federal Aviation, September 13, 2013
- DOD5030.61 DoD Airworthiness Policy, May 24, 2013, Incorporating Change 2, August 24, 2017
- DODD 5100.01 Functions of the Department of Defense and Its Major Components, 21 December 2010, Incorporating Change 1, September 17, 2020
- DODD 5100.19 Implementation of National Security Council Intelligence Directive No. 7 [SECRET] 19 March 1959
- DODD 5100.20 National Security Agency / Central Security Service, 26 January 2010
- DODD 5100.23: Administrative Arrangements for the National Security Agency, May 17, 1967, thru Ch 2, November 1, 1985
- DODD 5100.46 Foreign Disaster Relief (FDR), July 6, 2012
- DODD 5100.47: National Cryptologic School, April 30, 1965
- DODD 5100.55 United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN), February 27, 2006
- DODD 5100.78: United States Port Security Program, August 25, 1986

- DODD 5100.85 Intelligence Systems Board (ISB) June 27, 1995
- DODD 5100.96 DoD Space Enterprise Governance and Principal DoD Space Advisor (PDSA), June 9, 2017
- DODD 5101.02E DoD Executive Agent (EA) for Space, January 25, 2013
- DODD 5101.17E Roles and Responsibilities Associated with the Recovery of Chemical Warfare Material, May 11, 2016, Incorporating Change 3, May 9, 2022
- DODD 5101.20E DoD Biological Select Agents and Toxins (BSAT) Biosafety and Biosecurity Program, January 25, 2019
- DODD 5101.21E DoD Executive Agent for Unified Platform and Joint Cyber Command and Control (JCC2), June 4, 2020
- DODD 5105.02 Deputy Secretary of Defense, February 11, 2021
- DODD 5105.07 Director, Defense Digital Service (DDS), January 5, 2017, change 1, effective December 4, 2019
- DODD 5105.20 Defense Representation, United States Mission to the North Atlantic Treaty Organization (USNATO) and Europe, June 27, 2013, Incorporating Change 1, Effective May 14, 2020
- DODD 5105.21 Defense Intelligence Agency, January 25, 2023
- DODD 5105.23 National Reconnaissance Office (NRO), June 28, 2011, Incorporating Change 1, Effective October 29, 2015
- DODD 5105.42 Defense Counterintelligence and Security Agency, January 16, 2025
- DODD 5105.56: Central Imagery Office, May 6, 1992 [reissued 23 October 1995, rescinded October 1996]
- DODD 5105.60 National Geospatial-Intelligence Agency (NGA), July 29, 2009
- DODD 5105.62 Defense Threat Reduction Agency (DTRA), April 24, 2013, Incorporating Change 1, November 10, 2015
- DODD 5105.64 Defense Contract Management Agency (DCMA), January 10, 2013
- DODD 5105.65 Defense Security Cooperation Agency (DSCA), October 26, 2012
- DODD 5105.67 Department of Defense Counterintelligence Field Activity (DoD CIFA), 19 February 2002
- DODD 5105.68 Pentagon Force Protection Agency (PFPA), 5 December 2013, Incorporating Change 2, Effective May 22, 2019
- DODD 5105.72 Defense Technology Security Administration (DTSA), April 26, 2016
- DODD 5105.73 Defense Technical Information Center (DTIC), May 2, 2013, Incorporating Change 1, October 25, 2017
- DODD 5105.74 Defense Media Activity, September 13, 2023
- DODD 5105.75 Department of Defense Operations at U.S. Embassies, December 21, 2007
- DODD 5105.76 Planning for Presidential Transitions and the Transition of Political Appointees and Other Officials, August 30, 2022, Change 1 effective February 3, 2023
- DODD 5105.85 Defense Innovation Unit (DIU), July 5, 2016, Incorporating Change 1, November 23, 2018
- DODD 5105.86 Director, Strategic Capabilities Office (SCO), November 14, 2016
- DODD 5105.87 Director, Defense Digital Service (DDS), January 5, 2017
- DODD O-5105.88 OSD Red Team (redacted), November 25, 2020
- DODD 5106.01 Inspector General of the Department of Defense (IG DoD), April 20, 2012, Incorporating Change 2, Effective May 29, 2020
- DODD 5106.04 Defense Inspectors General, May 22, 2014, Incorporating Change 1, Effective May 14, 2020
- DODD 5110.10 Defense POW/MIA Accounting Agency (DPAA), January 13, 2017
- DODD 5111.01 Under Secretary of Defense for Policy (USD(P)), June 23, 2020
- DODD 5111.03 Deputy Under Secretary of Defense for Policy (DUSD(P)), 25 January 2017, Incorporating Change 1, April 14, 2020
- DODD 5111.07 Assistant Secretary of Defense for International Security Affairs (ASD(ISA)), 7 November 2008
- DODD 5111.10 Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, May 5, 2021
- DODD 5111.11 Director of Net Assessment, April 14, 2020
- DODD 5111.13 Assistant Secretary of Defense for Homeland Defense and Global Security (ASD(HD&GS)), March 23, 2018
- DODD 5111.14 Assistant Secretary of Defense for International Security Policy (ASD(ISP)), 22 March 2005
- DODD 5111.17 Assistant Secretary of Defense for Asian and Pacific Security Affairs (ASD(APSA)), 29 October 2008
- DODD 5111.18 Assistant Secretary of Defense for Global Strategic Affairs (ASD(GSA)), 13 June 2011
- DODD 5111.21 Arms Transfer and Technology Release Senior Steering Group and Technology Security and Foreign Disclosure Office, October 14, 2014, Incorporating Change 1, Effective July 14, 2020
- DODD 5122.05 Assistant Secretary of Defense for Public Affairs (ASD(PA)), August 7, 2017
- DODD 5132.03 Security Cooperation, January 16, 2025
- DODD 5134.08 Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs (ASD(NCB)), January 14, 2009, Incorporating Change 3, Effective March 27, 2019
- DODD 5134.10 Defense Advanced Research Projects Agency (DARPA), May 7, 2013, Incorporating Change 1, September 22, 2017

- DODD 5134.14 Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics (PDUSD(AT&L)), December 29, 2010, incorporating Change 1, May 4, 2011
- DODD 5134.09 Missile Defense Agency (MDA), September 17, 2009
- DODD 5135.02 Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), July 15, 2020
- DODD 5135.03 Deputy Under Secretary of Defense for Acquisition and Sustainment, December 10, 2020
- DODD 5137.02 Under Secretary of Defense for Research and Engineering (USD(R&E)), July 15, 2020
- DODD 5137.03 Deputy Under Secretary of Defense for Research and Engineering, December 10, 2020
- DODD 5143.01 Under Secretary of Defense for Intelligence and Security (USD(I&S)), October 24, 2014, Incorporating Change 2, April 6, 2020
- DODD 5143.02 Deputy Under Secretary of Defense for Intelligence and Security (DUSD(I&S)), January 29, 2020
- DODD 5144.02 DoD Chief Information Officer (DoD CIO), November 21, 2014, Incorporating Change 1, September 19, 2017
- DODD 5145.01 General Counsel of the Department of Defense (GC DoD), December 2, 2013, Incorporating Change 2, Effective January 30, 2015
- DODD 5148.11: Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), April 24, 2013
- DODD 5148.13: Intelligence Oversight, April 26, 2017
- DODD 5160.05E Roles and Responsibilities Associated with the Chemical and Biological Defense Program, November 12, 2024
- DODD 5160.41E Defense Language, Regional Expertise, and Culture (LREC) Program, August 21, 2015, Incorporating Change 2, Effective August 25, 2020
- DODD 5200.1-R Information Security Program Regulation, January 1997 (superseded by DoD Manual 5200.01, 4 volumes, February 2012)
- DODD 5200.2-R DoD Personnel Security Program, January 1987 (with Change 3, 23 Feb 1996) (superseded by DOD Manual 5200.02)
- DODD 5200.5 Communications Security (COMSEC) (CONFIDENTIAL), 6 October 1981
- DODD 5200.12 Conduct of Classified Meetings, 27 July 1992
- DODD 5200.17 The Security, Use and Dissemination of Communications Intelligence (COMINT) [SECRET] 26 January 1965
- DODD 5200.19, Control of Compromising Emanations [SECRET], 10 February 10, 1968
- DODD 5200.26 Defense Investigative Program, 12 June 1979
- DODD 5200.27: Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense, January 7, 1980
- DODD 5200.28 Security Requirements for Automated Information Systems (AISs), March 21, 1988.
- DODD 5200.30:Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records, March 21, 1983
- DODD 5200.31E, DoD Military Working Dog (MWD) Program, 10 August 2011, Incorporating Change 1, Effective September 21, 2020
- DODD 5200.32, Department of Defense Security Countermeasures (SCM) and Polygraph Education, Training, and Program Support, 26 February 1996
- DODD 5200.33 Defense Courier Service (DCS), 25 August 1998
- DODD 5200.37 Defense Human Intelligence, 16 January 2025
- DODD 5200.43, Management of the Defense Security Enterprise, October 1, 2012, Incorporating Change 3, July 14, 2020
- DODD 5200.47E, Anti-Tamper (AT), September 4, 2015, Incorporating Change 3, December 22, 2020

- DODD 5205.02E DoD Operations Security (OPSEC) Program, June 20, 2012, Incorporating Change 2, August 20, 2020
- DODD 5205.07 Special Access Program (SAP) Policy, September 12, 2024
- DOD Manual 5205.07 volume 1 DoD Special Access Program (SAP) Security Manual: General Procedures, updated January 17, 2025
- DOD Manual 5205.07 volume 2 DoD Special Access Program (SAP) Security Manual: Personnel Security, November 24, 2015, Incorporating Change 2, Effective October 30, 2020
- DOD Manual 5205.07 volume 3 DoD Special Access Program (SAP) Security Manual: Physical Security, April 23, 2015, Incorporating Change 3, Effective December 8, 2020
- DOD Manual 5205.07 volume 4 Special Access Program (SAP) Security Manual: Marking, October 10, 2013, Incorporating Change 1, Effective May 9, 2018
- DODD 5205.10 Department of Defense Treaty Inspection Readiness Program (DTIRP), December 5, 2000

- DODD 5205.12 Military Intelligence Program, November 27, 2024
- DODD 5205.14 DoD Counter Threat Finance (CTF), August 19, 2010, Incorporating Change 3, May 4, 2017
- DODD 5205.15E DoD Forensic Enterprise (DFE), April 26, 2011, Incorporating Change 1, August 14, 2017
- DODD 5205.82 Defense Institution Building, January 27, 2016, Change 1, effective May 4, 2017

- DODD-5210.2 Access to and Dissemination of Restricted Data, Change 3 - 16 November 1994
- DODD 5210.45: Personnel Security in the National Security Agency, May 9, 1964
- DODD 5210.46 DoD Building Security for the National Capital Region, January 28, 1982
- DODD 5210.48 Credibility Assessment (CA) Program, April 24, 2015, Incorporating Change 2, Effective October 1, 2020
- DODD 5210.50 Management of Serious Security Incidents Involving Classified Information, October 27, 2014, Incorporating Change 2, Effective September 18, 2020
- DODD 5210.52 Security Classification of Airborne Sensor Imagery and Imaging Systems, 18 May 1989
- DODD 5210.55 Department of Defense Presidential Support Program, 15 December 1998
- DODD 5210.56 Arming and the Use of Forece, November 18, 2016, with Change 1 effective November 6, 2020
- DODD 5210.70 DoD Cryptologic Training, 3 November 1980
- DODD 5210.78: Department of Defense Polygraph Institute (DoDPI), September 18, 1991
- DODD 5210.79 Defense Personnel Security Research and Education Center (PERSEREC), 31 May 1989
- DODD 5210.88 Safeguarding Biological Select Agents and Toxins, February 11, 2004

- DODD 5215.1 Computer Security Evaluation Center, 16 November 1994

- DODD 5220.6 Defense Industrial Personnel Security Clearance Review Program, 20 April 1999
- DODD 5220.22 National Industrial Security Program, 27 September 2004
- DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), February 2006, Incorporating Change 2, May 18, 2016
- NISPOM Supplement, DoD 5220.22-M-Sup. 1, February 1995
- Defense Department Overprint to the National Industrial Security Program Operating Manual Supplement, January 1998
- DOD Manual 5220.32, volume 1, National Industrial Security Program: Industrial Security Procedures for Government Activities, August 1, 2018, Incorporating Change 2, December 10, 2021
- DOD Manual 5220.32, volume 2, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI), April 17, 2014, Incorporating Change 2, December 10, 2021
- DODD 5230.11 Disclosure of Classified Military Information to Foreign Governments and International Organizations, 16 June 1992
- DODD 5230.20 Visits, Assignments, and Exchanges of Foreign Nationals, August 12, 1998
- DODD 5230.21 Protection of Classified National Security Council and Intelligence Information, 15 March 1982
- DODD 5230.23 Intelligence Disclosure Policy [CONFIDENTIAL] 18 November 1983
- DODD 5230.25 Withholding of Unclassified Technical Data From Public Disclosure, Administrative Reissuance, 18 August 1995
- DoD Manual 5230.30 DoD Mandatory Declassification Review (MDR) Program, December 22, 2011, Incorporating Change 3, Effective February 8, 2022

- DOD Manual 5240.01 Procedures Governing the Conduct of DoD Intelligence Activities, August 8, 2016 (with accompanying Fact Sheet)
- DOD Manual S-5240.01-A Procedures Governing the Conduct of DoD Intelligence Activities: Annex Governing Signals Intelligence Information and Data Collected Pursuant to Section 1.7(C) of E.O. 12333, January 7, 2021
- DODD 5240.01: DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities, September 27, 2024
    - DODD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons," December 1982, Incorporating Change 2, Effective April 26, 2017 (cancelled and incorporated into Directive 5240.01)
- DODD 5240.02: Counterintelligence (CI), March 17, 2015, Incorporating Change 1, Effective May 16, 2018
- DODD 5240.3: Counterintelligence and Operations Security Support Program for the Defense Nuclear Agency, January 25, 1983
- DODD 5240.06: Counterintelligence Awareness and Reporting, 17 May 2011, Incorporating Change 3, Effective August 31, 2020
- DODD 5240.9 Support to Department of Defense Offensive Counterintelligence Operations [SECRET] 28 November 1989
- DODD 5240.12 Department of Defense (DoD) Intelligence Commercial Activities (ICAs) July 1, 1996, updated January 11, 1999
- DODD 5240.19 Counterintelligence Support to the Defense Critical Infrastructure Program, 27 August 2007
- DODD 5250.01 Management of Intelligence Mission Data (IMD) in DoD Acquisition, January 22, 2013, Incorporating Change 1, August 29, 2017

- DODD 5400.07 DOD Freedom of Information Act Program, April 5, 2019
    - DOD Manual 5400.07 DOD Freedom of Information Act (FOIA) Program, January 25, 2017

- DODD 5505.06 Investigations of Allegations Against Senior DoD Officials, June 6, 2013
- DODD 5505.09 Interception of Wire, Electronic, and Oral Communications for Law Enforcement, April 20, 1995
- DODD 5535.02 DoD Patent Security Review Process, 24 March 2010

- DODD 6055.9E Explosives Safety Management and the DoD Explosives Safety Board, 19 August 2005
- DoD Biosurveillance, September 17, 2020, Change 1, June 21, 2024
- DODD 6490.14 Defense Suicide Prevention Program, June 18, 2013, Incorporating Change 1, Effective April 1, 2016

- DODD 7045.14 The Planning, Programming, Budgeting, and Execution (PPBE) Process, January 25, 2013, Incorporating Change 1, August 29, 2017
- DODD 7050.06 Military Whistleblower Protection, April 17, 2015, Incorporating Change 1, October 12, 2021
- DODD 7920.1, Life Cycle Management of Automated Information Systems (AIS), 17 October 1978

- DODD 8000.01 Management of the Department of Defense Information Enterprise (DoD IE), March 17, 2016
- DODD 8100.2 Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), April 14, 2004
- DODD 8140.01 Cyberspace Workforce Management, October 5, 2020
- DODD 8260.05 Support for Strategic Analysis (SSA), July 20, 2011
- DODD 8320.03 Unique Identification (UID) Standards for a Net-Centric Department of Defense, 23 March 2007
- DODD 8521.01E DoD Biometrics, January 13, 2016, Incorporating Change 1, August 15, 2017
- DODD 8520.1 Protection of Sensitive Compartmented Information (SCI), December 20, 2001
- DODD 8910.1 Management and Control of Information Requirements, 11 June 1993

DOD Instructions

- DODI 1000.01 Identification (ID) Cards Required by the Geneva Conventions, April 16, 2012
- DODI 1000.25 DoD Personnel Identity Protection (PIP) Program, March 2, 2016
- DODI 1000.29 DoD Civil Liberties Program, May 17, 2012, Incorporating Change 1, November 26, 2014
- DODI 1000.32 Prohibition of Lobbying Activity by Former DoD Senior Officials, March 26, 2020
- DODI 1005.06 Display of the National Flag at Half-staff, July 17, 2015
- DODI 1025.2, National Security Education Program, March 9, 2006
- DODI 1025.3 Administrator, National Security Education Program, May 13, 1994
- DODI 1025.5 National Security Education Program (NSEP) Grants to Institutions of Higher Education, February 13, 1995
- DODI 1025.11, DoD Science, Technology, Engineering, and Mathematics (STEM) Education Programs and Activities, August 21, 2020
- DODI 1100.22 Policy and Procedures for Determining Workforce Mix, January 8, 2008, April 12, 2010
- DODI 1300.06 Conscientious Objectors, July 12, 2017
- DODI 1300.17 Religious Liberty in the Military Services, September 1, 2020
- DODI 1300.18 Department of Defense (DoD) Personnel Casualty Matters, Policies, and Procedures, January 8, 2008, incorporating change 1, August 14, 2009
- DODI 1300.28 In-Service Transition for Transgender Service Members, Effective April 30, 2021
- DODI 1304.23 Acquisition and Use of Criminal History Record Information for Military Recruiting Purposes, October 7, 2005
- DODI 1315.20 Management of the DoD Foreign Area Officer Program, March 25, 2022
- DODI 1325.02 Desertion and Unauthorized Absence or Absence Without Leave, October 26, 2021
- DODI 1325.06 Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces, November 27, 2009, Incorporating Change 2, Effective December 20, 2021
- DODI 1325.07 Administration of Military Correctional Facilities and Clemency and Parole Authority, March 11, 2013
- DODI 1340.27 Military Foreign Language Skill Proficiency Bonuses, August 17, 2022
- DODI 1341.08 Payment of Death Gratuity to Survivors of Certain DoD Personnel Assigned to Intelligence Duties, 25 August 2006, Incorporating Change 1, Effective August 20, 2020
- DODI 1400.36 DoD Implementation of the Joint Intelligence Community Duty Assignment (JDA) Program, 2 Jun 2008, Incorporating Change 1, Effective October 5, 2020
- DODI 1430.16 Growing Civilian Leaders, August 23, 2022
- DODI 2000.03 International Interchange of Patent Rights and Technical Information, January 17, 2006, certified current as of December 3, 2010
- DODI 2000.11 Procedures for Handling Requests for Asylum and Temporary Refuge, May 13, 2010
- DODI 2000.12 DoD Antiterrorism (AT) Program, March 1, 2012, Incorporating Change 3, May 8, 2017

- DODI 2000.16 DoD AntiTerrorism Standards, October 2, 2006
- DODI 2000.21 DoD Support to International Chemical, Biological, Radiological, and Nuclear (CBRN) Incidents, April 5, 2016, Incorporating Change 1, May 8, 2017
- DODI 2000.25 DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS), December 16, 2021 with Change 1, May 27, 2022
- DODI 2000.26 DoD Use of the Federal Bureau of Investigation (FBI) eGuardian System, December 4, 2019
- DODI 2000.28 DoD Policy and Responsibilities Relating to the Regional Defense Combating Terrorism Fellowship Program (CTFP), November 14, 2013
- DODI 2000.30 Global Health Engagement (GHE) Activities, July 12, 2017
- DODI 2030.08 Implementation of Trade Security Controls (TSC) for Transfers of DoD U.S. Munitions List (USML) and Commerce Control List (CCL) Personal Property to Parties Outside DoD Control, May 23, 2006
- DODI 2040.02 International Transfers of Technology, Articles, and Services, July 10, 2008
- DODI 2040.03 End Use Certificates (EUCs), July 15, 2020
- DODI 2060.03 Application of the National Security Exclusion to the Agreements Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States of America, September 10, 2019
- DODI 2200.01 Combating Trafficking in Persons (CTIP), June 21, 2019
- DODI 2205.02 Humanitarian and Civic Assistance (HCA) Activities, June 23, 2014, Incorporating Change 1, May 22, 2017
- DODI 2310.08 Medical Program Support for Detainee Operations, September 5, 2019, with Change 1, effective August 25, 2021
- DODI 2310.09 Behavioral Science Support (BSS) for Detainee Operations and Intelligence Interrogations, September 5, 2019
- DODI 3000.05 Stability Operations, September 16, 2009, Incorporating Change 1, June 29, 2017
- DODI 3000.11 Management of DoD Irregular Warfare (IW) and Security Force Assistance (SFA) Capabilities, May 3, 2016
- DODI 3000.12 Management of U.S. Global Defense Posture (GDP), May 6, 2016, Incorporating Change 1, May 8, 2017
- DODI 3000.14 DoD Counterdrug and Counter-Transnational Organized Crime Policy, August 28, 2020
- DODI 3000.17 Civilian Harm Mitigation and Response, December 21, 2023
- DODI 3001.02 Personnel Accountability in Conjunction With Natural or Manmade Disasters, May 3, 2010
- DODI 3002.02 Personnel Recovery and 406 MHz Search and Rescue (SAR) Emergency Beacons in the Department of Defense, January 11, 2013, Incorporating Change 1, Effective April 25, 2016
- DODI 3002.03 DoD Personnel Recovery -- Reintegration of Recovered Personnel, July 15, 2013, Incorporating Change 1, April 26, 2016
- DoDI 3020.26 DoD Continuity Policy, June 4, 2024
- DODI 3020.39 Mission Assurance Policy for the Defense Intelligence Enterprise (DIE), March 2, 2015, Incorporating Change 2, Effective September 21, 2020
- DODI 3020.41 Contractor Personnel Authorized to Accompany the U.S. Armed Forces, October 3, 2005
- DODI 3020.42 Defense Continuity Plan Development, February 17, 2006
- DODI 3020.45 Defense Critical Infrastructure Program (DCIP) Management, April 21, 2006, Incorporating Change 1, June 6, 2017
- DODI 3020.46 The Militarily Critical Technologies List (MCTL), October 24, 2008, Incorporating Change 1, November 16, 2017
- DODI 3020.47 DoD Participation in the National Exercise Program (NEP), January 29, 2019
- DODI 3020.48 Guidance for Maritime Operational Threat Response (MOTR)-Related Conferencing Coordination Activities Implementation, March 6, 2009, Incorporating Change 1, Effective February 26, 2014, Certified current through March 6, 2016
- DODI 3020.50 Private Security Contractors Operating in Contingency Operations, Humanitarian or Peace Operations, or Other Military Operations or Exercises, October 13, 2022
- DODI 3020.51 Intelligence Support to the Defense Critical Infrastructure Program (DCIP), June 23, 2011, Incorporating Change 2, Effective July 9, 2020
- DODI 3020.52 DoD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards, May 18, 2012
- DODI 3025.19 Procedures for Sharing Information with and Providing Support to the U.S. Secret Service (USSS), Department of Homeland Security (DHS), November 29, 2011, Incorporating Change 1, March 13, 2017
- DODI 3025.20 Defense Support of Special Events, April 6, 2012, Incorporating Change 1, May 24, 2017
- DODI 3025.21 Defense Support of Civilian Law Enforcement Agencies, February 27, 2013, Incorporating Change 1, Effective February 8, 2019
- DODI 3025.23 Domestic Defense Liaison with Civil Authorities, May 25, 2016
- DODI 3100.08 The Technical Cooperation Program (TTCP), August 7, 2012, Incorporating Change 1, November 30, 2017

- DODI 3100.11 Management of Laser Illumination of Objects in Space, October 24, 2016
- DODI 3115.08 Collection of Information on Non-U.S. Persons Outside the United States at the Request of U.S. Law Enforcement Agencies (LEAs), January 14, 2009, Incorporating Change 3, Effective October 1, 2020
- DODI 3115.10E Intelligence Support to Personnel Recovery, March 24, 2006, Incorporating Change 1, November 6, 2020
- DODI 3115.11 DoD Intelligence Human Capital Management Operations, January 22, 2009, Incorporating Change 3, September 21, 2020
- DODI 3115.12 Open Source Intelligence (OSINT), August 24, 2010, Incorporating Change 2, Effective July 16, 2020
- DODI 3115.14 Civil Aviation Intelligence, July 29, 2011, Incorporating Change 2, Effective August 25, 2020
- DODI 3115.15 Geospatial Intelligence (GEOINT), December 6, 2011, Incorporating Change 2, Effective October 1, 2020
- DODI 3115.17 Management and Oversight of DoD All-Source Analysis, November 16, 2016, Incorporating Change 1, Effective September 21, 2020
- DODI 3115.19 Executive Agent for Tactical Exploitation of National Capabilities, February 7, 2023
- DODI 3150.02 DoD Nuclear Weapon Systems Surety Program, December 17, 2024
- DODI 3150.09 The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy, April 8, 2015, Incorporating Change 4, December 8, 2023
- DODI 3150.10 DoD Response to U.S. Nuclear Weapon Incidents, July 2, 2010
- DODI 3200.12 DoD Scientific and Technical Information Program (STIP), August 22, 2013, Incorporating Change 3, Effective December 17, 2018
- DODI 3200.19 Non-Lethal Weapons (NLW) Human Effects Characterization, May 17, 2012, Incorporating Change 1, September 13, 2017
- DODI 3200.20 Scientific and Engineering Integrity, July 26, 2012, Incorporating Change 1, December 5, 2017
- DODI 3201.01 Management of DoD Research and Development (R&D) Laboratories, September 29, 2016, with Change 1, December 8, 2017
- DODI 3201.04 In-House Laboratory Independent Research (ILIR) Program, October 18, 2013
- DODI 3201.05 Management of Science and Technology Reinvention Laboratory Personnel Demonstration Projects, December 29, 2021
- DODI 3204.01 DoD Policy for Oversight of Independent Research and Development (IR&D), August 20, 2014, Incorporating Change 2, July 9, 2020
- DODI 3216.01 Use of Animals in DoD Conducted and Supported Research and Training, March 20, 2019
- DODI 3216.02 Protection of Human Subjects and Adherence to Ethical Standards in DoD-Conducted and -Supported Research, April 15, 2020, with Change 1, June 29, 2022
- DODI 3222.03 DoD Electromagnetic Environmental Effects (E3) Program, August 25, 2014, Incorporating Change 2, October 10, 2017
- DODI 3300.2: Combined Intelligence Publishing Service (CIPS), February 7, 1994
- DODI 3300.05 Reserve Component Intelligence Enterprise (RCIE) Management, July 17, 2013, Incorporating Change 2, Effective August 7, 2020
- DODI 3300.07 Defense Intelligence Foreign Language and Regional and Culture Capabilities, February 14, 2017, Change 3 Effective May 18, 2022
- DODI 3305.01 National Intelligence University, January 24, 2017, Change 2, August 25, 2020
- DODI 3305.02 DoD General Intelligence Training and Certification, August 12, 2015, Incorporating Change 2, Effective September 28, 2020
- DODI 3305.09 DoD Cryptologic Training, June 13, 2013, Incorporating Change 2, Effective September 21, 2020
- DODI 3305.10: Geospatial-Intelligence (GEOINT) Training, July 3, 2013, Incorporating Change 2, Effective September 25, 2020
- DODI 3305.11: DoD Counterintelligence (CI) Training and Certification, August 13, 2015, Incorporating Change 2, Effective August 27, 2020
- DODI 3305.12: Intelligence and Counterintelligence (I&CI) Training of Non-U.S. Persons, October 14, 2016, Incorporating Change 2, Effective October 19, 2020
- DODI 3305.14: Joint Intelligence Training (JIT) and Certification, August 18, 2015, Incorporating Change 2, Effective September 25, 2020
- DODI 3305.15: DoD Human Intelligence (HUMINT) Training and Certification, August 13, 2015, Incorporating Change 2, Effective August 25, 2020
- DODI 3305.16: DoD Measurement and Signature Intelligence (MASINT) Training and Certification, August 13, 2015, Incorporating Change 2, Effective October 1, 2020
- DODI 3325.08: DoD Intelligence Collection Management, September 17, 2012, Incorporating Change 3, Effective August 26, 2020
- DODI 3325.11: Management of the Joint Reserve Intelligence Program (JRIP), June 26, 2015, Incorporating Change 2, Effective September 24, 2020

- DODI 3608.12: Joint Information Operations (IO) Education, November 4, 2005, incorporating Change 1, December 6, 2011
- DODI 3710.01: National Leadership Command Capabilities (NLCC) Configuration Management (CM), May 1, 2013
- DODI 3741.01: National Leadership Command Capabilities (NLCC) Configuration Management (CM), May 1, 2013, Incorporating Change 1, Effective July 15, 2020
- DODI 3901.01: Special Operations Policy and Oversight Council, December 26, 2023
- DODI 3902.01 Special Operations Forces: Joint Combined Exchange Training Program, November 16, 2023
- DODI 3902.02 Special Operations Forces Foreign Language, Regional Expertise, and Culture Policy, August 17, 2023
- DODI 4000.19 Interservice and Intragovernmental Support, August 9, 1995
- DODI 4120.15 Designating and Naming Military Aerospace Vehicles, November 2, 2023
- DODI 4140.01 DoD Supply Chain Materiel Management Policy, March 6, 2019
- DODI 4140.66 Registration and End-Use Monitoring of Defense Articles and/or Defense Services, September 7, 2010, Incorporating Change 1, May 24, 2017
- DODI 4140.67 DoD Counterfeit Prevention Policy, April 26, 2013, Incorporating Change 3, March 6, 2020
- DODI 4160.28 DoD Demilitarization Program, November 30, 2022
- DODI 4540.01 Use of International Airspace by U.S. Military Aircraft and for Missile and Projectile Firings, June 2, 2015
- DODI 4540.05 DoD Transportation of U.S. Nuclear Weapons, June 23, 2011, Incorporating Change 3, November 9, 2017
- DODI 4540.07 Telecommunications Services in the National Capital Region (NCR), September 24, 2009, Incorporating Change 2, August 10, 2012
- DODI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum, January 9, 2009
- DODI 4650.02 Military Auxiliary Radio System, December 20, 2021
- DODI 4650.06 Positioning, Navigation, and Timing Management, July 30, 2020, with Change 1, May 7, 2021
- DODI 4650.08 Positioning, Navigation, and Timing (PNT) and Navigation Warfare, December 27, 2018, with Change 1, December 30, 2020
- DODI 4715.06 Environmental Compliance in the United States, May 4, 2015, Incorporating Change 1, October 27, 2017
- DODI 4715.18 Emerging Chemicals of Environmental Concern, September 4, 2019, with Change 1, February 9, 2024
- DODI 4715.19 Use of Open-Air Burn Pits in Contingency Operations, November 13, 2018
- DODI 4715.27 DoD Low-Level Radioactive Waste (LLRW) Program, July 7, 2017, Incorporating Change 2, Effective April 12, 2019
- DODI 5000.02 Operation of the Defense Acquisition System, January 7, 2015, Incorporating Change 10, December 31, 2020
- DODI 5000.56 Programming Geospatial-Intelligence (GEOINT), Geospatial Information and Services (GI&S), and Geodesy Requirements for Developing Systems, July 9, 2010, Incorporating Change 2, Effective August 26, 2020
- DODI 5000.60 Defense Industrial Base Assessments, July 18, 2014, Incorporating Change 3, August 5, 2022
- DODI 5000.61 DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A), December 9. 2009
- DODI 5000.69 Joint Services Weapon and Laser System Safety Review Processes, August 10, 2023
- DODI 5000.73 Cost Analysis Guidance and Procedures, March 13, 2020
- DODI 5000.77 DoD Federally Funded Research and Development Center (FFRDC) Program, January 31, 2018, Incorporating Change 2, November 6, 2019
- DODI 5000.82 Requirements for the Acquisition of Digital Capabilities, June 1, 2023
- DODI 5000.83 Technology and Program Protection to Maintain Technological Advantage, July 20, 2020, with Change 1, effective May 21, 2021
- DODI 5000.86 Acquisition Intelligence, September 11, 2020
- DODI 5000.88 Engineering of Defense Systems, November 18, 2020
- DODI 5000.89 Test and Evaluation, November 19, 2020
- DODI 5000.90 Cybersecurity for Acquisition Decision Authorities and Program Managers, December 31, 2020
- DODI 5000.94 Use of Robotic Systems for Manufacture and Sustainment in the DoD, March 28, 2022
- DODI 5000.97 Digital Engineering, December 21, 2023
- DODI 5015.02 DoD Records Management Program, February 24, 2015, Incorporating Change 1, August 17, 2017
- DODI 5025.01 DoD Issuances Program, August 1, 2016, with Change 4, effective June 7, 2023
- DODI 5025.12 Standardization of Military and Associated Terminology, March 5, 2020, with Change 1, January 21, 2022

- DODI 5030.14 Disclosure of Atomic Information to Foreign Governments and Regional Defense Organizations, August 17, 2011, Incorporating Change 3, Effective May 28, 2020
- DODI 5030.36 Emergency Security Control of Air Traffic (ESCAT), April 24, 2014
- DODI 5030.57 Special Warnings to Mariners, December 5, 2011, Incorporating Change 2, Effective October 29, 2020
- DODI 5030.59 National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION Geospatial Intelligence, March 10, 2015, Incorporating Change 2, Effective September 24, 2020
- DODI 5040.02 Visual Information, October 27, 2011, Incorporating Change 2, Effective April 23, 2018
- DODI 5040.05 Alteration of Official DoD Imagery, June 6, 2006
- DODI 5100.76 Safeguarding Conventional Arms, Ammunition, and Explosives (AA&E), May 20, 2010, Incorporating Change 2, Effective October 19, 2020
- DODI 5100.86 DoD Forensic Science Committee, April 18, 2014
- DODI 5100.91 Joint Intelligence Interoperability Board (JIIB), October 28, 2008
- DODI C-5105.32 Defense Attache System (DAS) (U), March 18, 2009
- DODI 5105.58: Measurement and Signature Intelligence (MASINT), April 22, 2009, Incorporating Change 2, Effective September 24, 2020
- DODI C-5105.81, Implementing Instructions for DoD Operations at U.S. Embassies (U), November 6, 2008
- DODI 5110.11, Raven Rock Mountain Complex (RRMC) [redacted], October 4, 2010
- DODI 5111.19: Section 2282 Global Train-and-Equip Authority, July 26, 2011, Incorporating Change 1, May 8, 2017
- DODI 5129.47: Center for Countermeasures, January 26, 2015
- DODI 5132.13: Staffing of Security Cooperation Organizations (SCOs) and the Selection and Training of Security Cooperation Personnel, January 9, 2009
- DODI 5132.14: Assessment, Monitoring, and Evaluation Policy for the Security Cooperation Enterprise, January 13, 2017
- DODI 5145.03: Oversight of the DoD Personnel Security Programs, January 10, 2013, Incorporating Change 1, Effective June 19, 2020
- DODI 5160.68: Single Manager for Conventional Ammunition (SMCA): Responsibilities of the SMCA, the Military Services, and United States Special Operations Command (USSOCOM), December 29, 2008
- DODI 5160.71: DoD Language Testing Program, June 30, 2022
- DODI 5200.01: DoD Information Security Program and Protection of Sensitive Compartmented Information, April 21, 2016, Incorporating Change 2, Effective October 1, 2020
- DODI 5200.02: DoD Personnel Security Program (PSP), March 21, 2014, Incorporating Change 3, Effective September 24, 2020
- DODI 5200.08: Security of DoD Installations and Resources, December 10, 2005, Incorporating Change 3, Effective November 20, 2015
- DODI 5200.33: Defense Courier Operations (DCO), June 30, 2011
- DODI 5200.39: Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E), May 28, 2015, Incorporating Change 3, Effective October 1, 2020
- DODI S-5200.42: Defense Human Intelligence (HUMINT) and Related Intelligence Activities (redacted), December 8, 2009
- DODI 5200.44: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, February 16, 2024
- DODI 5200.46: DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC), September 9, 2014, Incorporating Change 1, Effective May 4, 2018
- DODI 5200.48: Controlled Unclassified Information (CUI), March 6, 2020
- DODI 5205.08: Access to U.S. Classified Cryptographic Information, February 16, 2018, Incorporating Change 1, September 24, 2020
- DODI 5205.10: DoD Treaty Inspection Readiness Program (DTIRP), February 20, 2009
- DODI 5205.11: Management, Administration, and Oversight of DoD Special Access Programs (SAPs), September 12, 2024
- DODI 5205.13: Defense Industrial Base (DIB) Cyber Security (CS) Activities, January 29, 2010, Incorporating Change 2, August 21, 2019
- DODI 5205.16 The DoD Insider Threat Program, December 20, 2024
- DODI 5205.83: DoD Insider Threat Management and Analysis Center (DITMAC), March 30, 2017, Incorporating Change 1 effective October 29, 2020
- DODI 5205.85: Enhanced Security Program to Support the DoD Innovation Initiative, August 16, 2022
- DODI 5205.87: Mitigating Risks Related to Foreign Ownership, Control, or Influence for Covered DoD Contractors and Subcontractors, May 13, 2024
- DODI 5210.02: Access to and Dissemination of Restricted Data and Formerly Restricted Data, June 3, 2011, Incorporating Change 1, October 25, 2017

- DODI 5210.42: DoD Nuclear Weapons Personnel Reliability Assurance, April 27, 2016, Incorporating Change 3, October 11, 2019
- DODI 5210.45: Personnel Security Policies and Procedures for Sensitive Cryptologic Information in the National Security Agency/Central Security Service, November 14, 2008, Certified Current Through November 14, 2015,Incorporating Change 3, Effective August 27, 2020
- DODI 5210.65: Security Standards for Safeguarding DoD Chemical Agents, October 1, 2020
- DODI 5210.83: DoD Unclassified Controlled Nuclear Information (UCNI), July 12, 2012, Incorporating Change 2, Effective October 2, 2020
- DODI 5210.87: Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs), November 30, 1998
- DODI 5210.88: Security Standards for Safeguarding Biological Select Agents and Toxins, May 26, 2020
- DODI 5210.89: Minimum Security Standards for Safeguarding Biological Select Agents and Toxins, April 18, 2006
- DODI 5210.91: Polygraph and Credibility Assessment (PCA) Procedures, August 12, 2010, Incorporating Change 2, Effective March 30, 2020
- DODI 5215.2 Computer Security Technical Vulnerability Reporting Program, 2 September 1986
- DODI 5220.22: National Industrial Security Program (NSIP), March 18, 2011, as amended (superseded by DODI 5220.31)
- DODI 5220.28 Application of Special Eligibility and Clearance Requirements in the SIOP-ESI Program for Contractor Employees, 8 March 1978
- DODI 5220.31 National Industrial Security Program, May 9, 2023
- DODI 5230.09 Clearance of DoD Information for Public Release, January 25, 2019, with Change 1, Effective February 9, 2022
- DODI 5230.16 Public Affairs Guidance for Nuclear Weapon and Radiological Material Incidents, October 24, 2023
- DODI 5230.21: Protection of Classified National Security Council and Intelligence Information, March 15, 1982
- DODI 5230.24 Distribution Statements on DoD Technical Information, January 10, 2023
- DODI 5230.27 Presentation of DoD-Related Scientific and Technical Papers at Meetings, November 18, 2016, Incorporating Change 1, September 15, 2017
- DODI 5230.29: Security and Policy Review of DoD Information for Public Release, August 13, 2014, Incorporating Change 2, February 8, 2022
- DODI 5240.04: Counterintelligence (CI) Investigations, April 1, 2016, Incorporating Change 2, Effective September 18, 2020
- DODI 5240.05: Technical Surveillance Countermeasures (TSCM), April 3, 2014, Incorporating Change 2, Effective August 27, 2020
- DODI S-5240.09, Offensive Counterintelligence Operations (OFCO) (U), October 29, 2008
- DODI 5240.10: Counterintelligence (CI) in the Combatant Commands and Other DoD Components, October 5, 2011, Incorporating Change 1, Effective October 15, 2013
- DODI 5240.16: DoD Counterintelligence Functional Services, August 27, 2012, Incorporating Change 1, Effective October 15, 2013
- DODI 5240.17: DoD Counterintelligence Collection Reporting, October 26, 2005
- DODI 5240.18: Counterintelligence (CI) Analysis and Production, November 17, 2009, Incorporating Change 3, Effective September 24, 2020
- DODI 5240.19: Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP), January 31, 2014, Incorporating Change 2, Effective November 6, 2020
- DODI 5240.22: Counterintelligence Support to Counterterrorism and Force Protection, October 12, 2022
- DODI 5240.25: Counterintelligence Badges and Credentials, March 30, 2012, Incorporating Change 2, Effective May 9, 2018
- DODI 5240.26: Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat, May 4, 2012, Incorporating Change 3, Effective December 7, 2020
- DODI 5240.27: Joint Counterintelligence Training Activity (JCITA), November 13, 2013, Incorporating Change 2, Effective October 2, 2020
- DODI 5250.11: Damage Assessments, December 23, 1991
- DODI 5400.04 Provision of Information to Congress, March 17, 2009
- DODI 5400.11 DoD Privacy and Civil Liberties Programs, January 29, 2019, with Change 1 effective December 8, 2020
    - DOD Manual 5400.11, volume 2 DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plans, May 6, 2021
- DODI 5400.13 Public Affairs (PA) Operations, October 15, 2008
- DODI 5400.14 Procedures for Joint Public Affairs Operations, November 3, 2014
- DODI 5400.16 DoD Privacy Impact Assessment (PIA) Guidance, July 14, 2015

- DODI 5400.17 Official Use of Social Media for Public Affairs Purposes, August 12, 2022, with Change 1 effective January 24, 2023
- DODI 5405.03 Development, Submission, and Approval of Proposed Public Affairs Guidance (PPAG), February 18, 2016
- DODI 5410.01 Release of Information Concerning Accidents Involving Military Personnel or Equipment or Concerning Senior Personnel, June 2, 2009
- DODI 5500.14 Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, May 27, 2010
- DODI 5505.03: Initiation of Investigations by Defense Criminal Investigative Organizations, March 24, 2011, Incorporating Change 2, February 13, 2017
- DODI 5505.09: Communication Interception for Law Enforcement, August 22, 2023
- DODI 5505.14: DNA Collection and Submission Requirements for Law Enforcement, April 5, 2022
- DODI 5505.15: DoD Contractor Disclosure Program, June 3, 2021, with Change 1, effective October 31, 2022
- DODI 5505.16: Criminal Investigations by Personnel Who Are Not Assigned to a Defense Criminal Investigative Organization, May 7, 2012
- DODI 5505.17: Personally Identifiable Information and Law Enforcement Information Handling by DoD Law Enforcement Activities, August 22, 2023
- DODI 5525.01: Foreign Criminal and Civil Jurisdiction, May 31, 2019
- DODI 5525.07: Implementation of the August 1984 Memorandum of Understanding (MOU) Between the Department of Justice (DOJ) and DOD Relating to the Investigation and Prosecution of Certain Crimes, March 5, 2020
- DODI 5525.13: Limitation of Authority to Deputize DoD Uniformed Law Enforcement Personnel by State and Local Governments, September 28, 2007, Incorporating Change 2, Effective September 8, 2020
- DODI 5525.14: DoD Law Enforcement Officers (LEOs) Flying Armed, March 22, 2011, Incorporating Change 4, Effective October 1, 2020
- DODI 5525.16: Law Enforcement Defense Data Exchange (LE D-DEx), August 29, 2013 Incorporating Change 3, Effective October 30, 2020
- DODI 5525.18: Law Enforcement Criminal Intelligence (CRIMINT) in DoD, October 18, 2013, Incorporating Change 3, Effective October 1, 2020
- DODI 5525.19: DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB), May 4, 2016, Incorporating Change 2, Effective October 1, 2020
- DODI 5530.03: International Agreements, December 4, 2019
- DODI 5535.10: Coordination of DoD Efforts to Identify, Evaluate, and Transfer DoD Technology Items, Equipment, and Services to Federal, State, and Local First Responders, November 24, 2009, Incorporating Change 1, May 24, 2017
- DODI 5535.11: Availability of Samples, Drawings, Information, Equipment, Materials, and Certain Services to Non-DoD Persons and Entities, March 19, 2012
- DODI 6000.16: Military Health Support for Stability Operations, May 17, 2010
- DODI 6050.05: DoD Hazard Communication (HAZCOM) Program, February 26, 2019
- DODI 6055.08: Occupational Ionizing Radiation Protection Program, April 9, 2021
- DODI 6055.11: Protecting Personnel from Electromagnetic Fields, May 12, 2021
- DODI 6055.15: DoD Laser Protection for Military Lasers, August 25, 2023
- DODI 6055.17: DoD Emergency Management (EM) Program, February 13, 2017, Incorporating Change 3, June 12, 2019
- DODI 6055.20: Assessment of Significant Long-Term Health Risks from Past Environmental Exposures on Military Installations, June 6, 2017, Incorporating Change 2, Effective June 10, 2019
- DODI 6420.01: National Center for Medical Intelligence (NCMI), March 20, 2009, Incorporating Change 3, Effective September 8, 2020
- DODI 6440.03: DoD Laboratory Network (DLN), June 10, 2011
- DODI 6490.05: Maintenance of Psychological Health in Military Operations, November 22, 2011, Incorporating Change 3, May 29, 2020
- DODI 7041.03: Economic Analysis for Decision-making, September 9, 2015, Incorporating Change 1, October 2, 2017
- DODI 7050.03: DoD Office of the Inspector General Access to Records and Information, November 13, 2024
- DODI 7600.02 Audit Policies, October 16, 2014, Incorporating Change 1, Effective March 15, 2016
- DODI 7650.01 Government Accountability Office (GAO) and Comptroller General Requests for Access to Records, January 27, 2009, Incorporating Change 2, Effective May 15, 2018
- DODI 7650.02 Engaging with the Government Accountability Office (GAO) on GAO Audits, January 24, 2020, with Change 1, January 26, 2022
- DODI 7650.03 Follow-up on Government Accountability Office (GAO), Inspector General of the Department of Defense (IG DoD), and Internal Audit Reports, 18 December 2014, Incorporating Change 1, Effective January

31, 2019
- DODI 8110.01 Mission Partner Environment Information Sharing Capability Implementation for the DoD, June 30, 2021
- DODI 8130.01 Installation Geospatial Information and Services (IGI&S), April 9, 2015
- DODI 8170.01 Online Information Management and Electronic Messaging, December 31, 2018
- DODI 8220.02: Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations, April 30, 2009
- DODI 8260.03: The Global Force Management Data Initiative (GFM DI), February 19, 2014, Incorporating Change 1, Effective March 19, 2018
- DODI 8260.04: Military Health System (MHS) Support to DoD Strategic Analysis, December 18, 2009
- DODI 8310.01: Information Technology Standards in the DoD, February 2, 2015
- DODI 8320.02: Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, August 5, 2013, Incorporating Change 1, Effective June 24, 2020
- DODI 8320.05: Electromagnetic Spectrum Data Sharing, August 18, 2011
- DODI 8320.07: Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, August 3, 2015, Incorporating Change 1, December 5, 2017
- DODI 8330.01: Interoperability of Information Technology, Including National Security Systems, September 27, 2022
- DODI 8410.01 Internet Domain Name and Internet Protocol Address Space Use and Approval, December 4, 2015, incorporating Change 1, June 4, 2021
- DODI 8410.02 Support to DoD Information Network Operations, December 8, 2021
- DODI 8420.02 DoD Satellite Communications, August 3, 2023
- DODI 8440.10 DoD Information Technology (IT) Service Management (ITSM), December 24, 2015
- DODI 8500.01 Cybersecurity, March 14, 2014, Incorporating Change 1, Effective October 7, 2019
- DODI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014, Incorporating Change 3, December 29, 2020
- DODI 8520.02 Public Key Infrastructure and Public Key Enabling, May 18, 2023
- DODI 8520.03 Identity Authentication for Information Systems, May 19, 2023
- DODI 8523.01 Communications Security (COMSEC), January 6, 2021
- DODI 8530.01 Cybersecurity Activities Support to DoD Information Network Operations, March 7, 2016, Incorporating Change 1, July 25, 2017
- DODI 8530.03 Cyber Incident Response, August 9, 2023
- DODI 8531.01 DoD Vulnerability Management, September 15, 2020
- DODI 8550.01 DoD Internet Services and Internet-Based Capabilities, September 11, 2012
- DODI 8560.01 Communications Security (COMSEC) Monitoring, August 22, 2018
- DODI 8580.02 Security of Individually Identifiable Health Information in DoD Health Care Programs, August 12, 2015
- DODI 8581.01 Information Assurance (IA) Policy for Space Systems Used by the Department of Defense, June 8, 2010
- DODI 8582.01 Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information, December 9, 2019
- DODI 8585.01 DoD Cyber Red Teams, January 11, 2024
- DODI 8910.01 Information Collection and Reporting, March 6, 2007, Incorporating Change 1, January 17, 2013

Other

- Prepublication and Security Review of Privately Written Works by Current and Former DoD Personnel, Directive-Type Memorandum (DTM) 24-005, November 8, 2024
- DoD Standards for Records Management Capabilities in Programs Including Information Technology, Directive-Type Memorandum (DTM) 22-001, March 3, 2022, Incorporating Change 1, February 22, 2023
- Tenets of Responsible Behavior in Space, memo from the Secretary of Defense, July 7, 2021
- Department of Defense Implementation of Internet Protocol Version 6, Directive-Type Memorandum (DTM) 21-004, January 29, 2021
- Federal Advisory Committee Management Program Ethics Responsibilities, Directive-Type Memorandum (DTM) 21-002, May 21, 2021, Incorporating Change 3, May 13, 2024
- DoD Public Web Program, Directive-Type Memorandum (DTM) 21-001, June 15, 2021, Incorporating Change 3, March 27, 2024
- Establishment of the Climate Working Group, March 9, 2021
- Special Access Program Contractor Portfolio Program Establishment, December 15, 2020 (via *Air Force Magazine*)
- Joint Identity Activities, Joint Doctrine Note 1-20, 24 November 2020

- Enabling Cyberspace Accountability of DoD Components and Information Systems, Directive-Type Memorandum (DTM) 20-004, November 13, 2020
- Procedures for the DOD Personnel Security Program (PSP), DOD Manual 5200.02, April 3, 2017, with change 1 effective October 29, 2020
- Interim Regulations for Condolence or Sympathy Payments to Friendly Civilians for Injury or Loss That Is Incident to Military Operations, Under Secretary of Defense, June 22, 2020
- Missile Defense System Policies and Governance, Directive-Type Memorandum 20-002, March 13, 2020, Incorporating Change 4, February 20, 2024
- Strategy, Joint Doctrine Note 2-19, December 10, 2019
- Interim Policy for DoD Intelligence Interrogations, Detainee Debriefings (I2D2), and Tactical Questioning (TQ), Directive-Type Memorandum (DTM) 19-010, September 6, 2019, Incorporating Change 1, Effective October 6, 2020
- Expedited Screening Protocol (ESP), Directive-Type Memorandum (DTM) 19-008, July 20, 2019, Incorporating Change 3, Effective August 26, 2021
- Competition Continuum, Joint Doctrine Note 1-19, June 3, 2019
- Physical Security Program: Access to DoD Installations, DoD Manual 5200.08, volume 3, January 2, 2019, Change 1, September 18, 2020
- Establishment of the Close Combat Lethality Task Force (CCLTF), Directive-Type Memorandum (DTM) 18-001, March 16, 2018, Incorporating Change 1, Effective December 28, 2018
- Prohibition on Providing Funds to the Enemy and Authorization of Additional Access to Records, Directive-Type Memorandum (DTM) 18-003, April 9, 2018, Incorporating Change 5, January 11, 2022
- Authority for Support of Special Operations for Irregular Warfare (IW), Directive-Type Memorandum (DTM) 18-005, August 3, 2018, Incorporating Change 03, August 19, 2021
- Interim Policy and Guidance for Defense Support to Cyber Incident Response, Directive-Type Memorandum (DTM) 17-007, June 21, 2017, Incorporating Change 7, October 18, 2023
- Guidance for the Domestic Use of Unmanned Aircraft Systems in U.S. National Airspace, DoD policy memorandum, August 18, 2018
- Joint Inspectors General Manual, DoD Manual 5106.06, May 7, 2018
- Strategy, Joint Doctrine Note 1-18, April 25, 2018
- DoD Security Accreditation and Certification, DoD Manual 3305.13, March 14, 2011, Incorporating Change 1, April 26, 2018
- Defense Demilitarization: Program Administration, DoD Manual 4160.28, Volume 1, August 9, 2017, Change 1, January 16, 2018
- Defense Demilitarization: Demilitarization Coding, DoD Manual 4160.28, Volume 2, March 9, 2017, Change 3, August 9, 2019
- Information Assurance Workforce Improvement Program, DoD 8570.01-M, December 19, 2005, Incorporating Change 4, November 10, 2015
- Disciplinary and Adverse Actions, Administrative Instruction 8, December 16, 2016
- Department of Defense Law of War Manual, DoD Office of General Counsel, June 2015, updated July 2023
- Joint Electromagnetic Spectrum Operations, Joint Doctrine Note 3-16, 20 October 2016
- Identity Activities, Joint Doctrine Note 2-16, 03 August 2016
- Office of the Secretary of Defense and Joint Staff (JS) Freedom of Information Act (FOIA) Program, Administrative Instruction 108, June 23, 2016, Incorporating Change 2, Effective February 9, 2022
- Command Red Team, Joint Doctrine Note 1-16, 16 May 2016
- Integrated DoD Intelligence Priorities, Directive-Type Memorandum (DTM) 15-004, September 3, 2015, Incorporating Change 2, Effective September 4, 2018
- Historical Research in the Files of the Office of the Secretary of Defense, Administrative Instruction 50, May 20, 2015, Incorporating Change 2, February 10, 2022
- DoD Intelligence and Security Training Standards, DoD Manual 3115.11, March 24, 2015, Incorporating Change 3, Effective October 29, 2020
- Guidance for the Domestic Use of Unmanned Aircraft Systems, Policy Memorandum 15-002, Deputy Secretary of Defense, February 17, 2015
- Policy Guidance for the Processing of National Interest Determinations (NIDs) in Connection with Foreign Ownership, Control, or Influence (FOCI), Directive-Type Memorandum (DTM) 15-002, February 11, 2015, Incorporating Change 7, Effective November 6, 2020
- DoD Compliance with Section 4 of Presidential Policy Directive-28, "Signals Intelligence Activity", memorandum from USD(I), January 20, 2015
- Nuclear Weapons Personnel Reliability Program, DoD Manual 5210.42, January 13, 2015, Incorporating Change 4, May 9, 2022
- DoD Nuclear Weapon System Safety Program Manual, DoD Manual 3150.02, January 31, 2014, Incorporating Change 4, May 7, 2021

- DoD Geospatial Intelligence (GEOINT) Accreditation and Certification, DoD Manual 3305.10, May 27, 2014, Incorporating Change 2, Effective September 14, 2020
- Cryptologic Accreditation and Certification, DoD Manual 3305.09, May 27, 2014, Incorporating Change 2, Effective October 1, 2020
- DoD Implementation of Presidential Policy Directive 19, Directive-Type Memorandum (DTM) 13-008, July 8, 2013, Incorporating Change 5, April 19, 2021
- Congressional Notification for Authorized Public Disclosure of Intelligence Information, Directive-Type Memorandum (DTM) 13-009, October 8, 2013
- DoD Internal Information Collections, Directive-Type Memorandum (DTM) 12-004, April 24, 2012, Incorporating Change 2, October 8, 2013
- Nuclear Weapon Accident Response Procedures (NARP), DoD Manual 3150.08, August 22, 2013, Incorporating Change 2, Effective July 21, 2020
- OSD Records and Information Management Program, Administrative Instruction 15, May 3, 2013, Incorporating Change 2, November 17, 2020
- Deviations from the DoD Physical Security Program, Directive-Type Memorandum (DTM) 13-005, April 25, 2013, Incorporating Change 3, Effective November 20, 2015
- Original Classification Authority and Writing a Security Classification Guide, DoD Manual 5200.45, January 17, 2025 (replaces DoD Handbook 5200.01H, November 1999)
- Use of Excess Ballistic Missiles for Space Launch, Directive-Type Memorandum (DTM) 11-008, July 5, 2011, Incorporating Change 3, April 25, 2013
- Mental Health Assessments for Members of the Military Services Deployed in Connection with a Contingency Operation, Directive-Type Memorandum (DTM) 11-011, August 12, 2011, incorporating Change 3, December 14, 2012
- Policy Guidance for Foreign Ownership, Control, or Influence (FOCI), Directive-Type Memorandum (DTM) 09-019, September 2, 2009, incorporating Change 6, January 9, 2014
- DoD Sensitive Compartmented Information (SCI) Administrative Security Manual, DoD Manual 5105.21, 3 volumes, October 19, 2012
  - Volume 1: Administration of Information and Information Systems Security
  - Volume 2: Administration of Physical Security, Visitor Control, and Technical Security
  - Volume 3: Administration of Personnel Security, Industrial Security, and Special Activities, Incorporating Change 2, Effective September 14, 2020
- Implementing Guidelines for Periodic Review of Detainees Held at Guantanamo Bay per Executive Order 13567, Directive-Type Memorandum (DTM) 12-005, May 9, 2012, Incorporating Change 2, November 4, 2013
- DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters, Directive-Type Memorandum (DTM) 08-052, June 17, 2009, incorporating Change 6, September 10, 2015 (cancelled and superseded by Directive 5148.13)
- Next Generation Common Access Card (CAC) Implementation Guidance, Directive-Type Memorandum (DTM) 08-003, December 1, 2008, incorporating Change 5, October 8, 2013
- DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12), Directive-Type Memorandum (DTM) 08-006, November 26, 2008, incorporating Change 5, October 8, 2013
- Intelligence Oversight Policy Guidance, Directive-Type Memorandum (DTM) 08-011, March 26, 2008, incorporating Change 6, September 10, 2015
- Declassification Marking Guidance for DoD Special Access Program (SAP) Classified Material, DTM 07-021, April 26, 2007
- Technology Security and Foreign Disclosure (TS&FD) Processes, Directive-Type Memorandum (DTM) 11-053, January 9, 2012, Incorporating Change 2, February 8, 2013 (expired)
- Videotaping or Otherwise Electronically Recording Strategic Intelligence Interrogations of Persons in the Custody of the Department of Defense, Directive-Type Memorandum (DTM) 09-031, May 10, 2010, Incorporating Change 3, May 25, 2012
- Responsible and Effective Use of Internet-based Capabilities, Directive-Type Memorandum (DTM) 09-026, February 25, 2010, incorporating Change 4, May 9, 2012
- Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems, Directive-Type Memorandum (DTM) 09-016, March 25, 2010, Incorporating Change 3, March 23, 2012
- Department of Defense Support to Foreign Disaster Relief, GTA-90-01-030, 13 July 2011
- Space Systems Acquisition Policy (SSAP), Directive-Type Memorandum (DTM) 09-025, October 18, 2010, incorporating Change 3, January 11, 2013
- Immediate Implementation Provisions of Executive Order 13526, 'Classified National Security Information', Directive-Type Memorandum (DTM) 11-004, April 26, 2011
- Control of NATO Classified Documents, Administrative Instruction 27, August 18, 2022
- Counterinsurgency (COIN) Training and Reporting Guidance for Preparing U.S. Forces to Succeed in Afghanistan and Pakistan, Directive-Type Memorandum (DTM) 11-002, December 9, 2010, incorporating Change 1, May 18, 2011

- Law Enforcement Reporting of Suspicious Activity, Directive-Type Memorandum (DTM) 10-018, October 1, 2010
- Interim Policy Guidance for DoD Physical Access Control, Directive-Type Memorandum (DTM) 09-012, December 8, 2009, Incorporating Change 9, August 23, 2018
- Policy Guidance for DoD Access Control, Directive-Type Memorandum (DTM) 08-004, April 9, 2008, Incorporating Change 3, March 19, 2013
- UCMJ Jurisdiction Over DoD Civilian Employees, DoD Contractor Personnel, and Other Persons Serving With or Accompanying the Armed Forces Overseas During Declared War and in Contingency Operations, Directive-Type Memorandum (DTM) 08-009, March 10, 2008, incorporating Change 1, September 23, 2010
- Intelligence Oversight Policy Guidance, Directive-Type Memorandum (DTM) 08-11, March 26, 2008, incorporating Change 1, September 8, 2010
- Fundamental Research, memorandum from Under Secretary of Defense Ashton B. Carter, May 24, 2010
- Law Enforcement Suspicious Activity Reporting (SAR) System - eGuardian, Secretary of Defense Robert M. Gates, May 20, 2010
- Safety Standards for Microbiological and Biomedical Laboratories, DoD Manual 6055.18-M, August 11, 2020
- Guide to Nongovernmental Organizations for the Military, Office of the Assistant Secretary of Defense (Health Affairs), Edited and rewritten by Lynn Lawry MD, Summer 2009
- Security of Unclassified DoD Information on Non-DoD Information Systems, Directive-Type Memorandum (DTM) 08-027, July 31, 2009, incorporating Change 1, September 16, 2010
- DoD Counterthreat Finance (CTF) Policy, Directive-Type Memorandum (DTM) 08-034, December 2, 2008
- DoD Operations Security (OPSEC) Program Manual, November 3, 2008, Incorporating Change 2, Effective October 29, 2020
- DOD Manual 3020.45, volume 1: Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP), October 24, 2008
- DOD Manual 3020.45, volume 2: Defense Critical Infrastructure Program (DCIP): DCIP Remediation Planning, October 28, 2008
- DoD Use of the Civil Search and Rescue Satellite-aided Tracking (SARSAT) System for Support to Personnel Recovery, Directive-Type Memorandum (DTM) 08-021, October 17, 2008, incorporating Change 1, September 16, 2010
- Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations, memorandum from the Secretary of Defense, June 23, 2009
- Establishment of the Defense Counterintelligence and Human Intelligence Center (DCHC), Directive-Type Memorandum 08-032, July 22, 2008
- DoD Force Protection Threat Information, Directive-Type Memorandum 08-007, July 22, 2008
- Reorganization of the Office of the Under Secretary of Defense for Intelligence, USD(I) Memorandum, June 18, 2008
- Report of the Overseas Jurisdiction Advisory Committee, the Advisory Committee on Criminal Law Jurisdiction Over Civilians Accompanying the Armed Forces in Time of Armed Conflict, April 1997
- Irregular Warfare (IW) Joint Operating Concept (JOC), version 1.0, 11 September 2007
- Joint Urban Operations Joint Integrating Concept, version 1, U.S. Joint Forces Command, July 23, 2007
- DoD 5200.08-R Physical Security Program, April 9, 2007, Incorporating Change 2, October 19, 2020
- An Assessment of International Legal Issues in Information Operations, DoD Office of General Counsel, May 1999

---

https://irp.fas.org/doddir/dod/
Created by John Pike
Maintained by Steven Aftergood
Updated June 26, 2024

FAS Note: Pursuant to DOD Instruction 2000.16 dated 14 Jun 01, the term "Terrorist Threat Condition" (THREATCON) has now been replaced by the term "Terrorist Force Protection Condition" (FPCON). Individual classifications and measures remain the same.

APPENDIX J

THREATCON SYSTEM

SECTION I. BASIC THREATCON PROCEDURES

1. General. The threat conditions (THREATCONs) outlined below describe the progressive level of a terrorist threat to all US military facilities and personnel under DOD Directive O-2000.12. As approved by the Chairman of the Joint Chiefs of Staff, the terminology and definitions are recommended security measures designed to ease inter-Service coordination and support of US military antiterrorism activities. The purpose of the THREATCON system is accessibility to, and easy dissemination of, appropriate information. The declaration, reduction, and cancellation of THREATCONs remain the exclusive responsibility of the commanders specified in the order. Although there is no direct correlation between threat information (e.g., Intelligence Summaries, Warning Reports, and Spot Reports) and THREATCONs, such information, coupled with the guidance provided below, assists commanders in making prudent THREATCON declarations. THREATCONs may also be suffixed with the geographic area deemed at risk. Once a THREATCON is declared, the selected security measures are implemented immediately. NOTE: When used in antiterrorism plans, recommend that the information contained in this appendix be marked "For Official Use Only" (FOUO) in accordance with DOD Regulation 5400.7-R, October 1990. The DOD Directive O-2000.12 recommended measures are:

a. THREATCON NORMAL exists when a general threat of possible terrorist activity exists but warrants only a routine security posture.
b. THREATCON ALPHA applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to implement certain measures from higher THREATCONs resulting from intelligence received or as a deterrent. The measures in this THREATCON must be capable of being maintained indefinitely.

(1) Measure 1. At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of US installations. Watch for abandoned parcels or suitcases and any unusual activity.

(2) Measure 2. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available.

(3) Measure 3. Secure buildings, rooms, and storage areas not in regular use.

(4) Measure 4. Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

(5) Measure 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

(6) Measure 6. As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO either individually or in combination with each other.

(7) Measure 7. Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher THREATCONs.

(8) Measure 8. Review and implement security measures for high-risk personnel as appropriate.

(9) Measure 9. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(10) Measure 10. To be determined.

c. THREATCON BRAVO applies when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

(1) Measure 11. Repeat measure 1 and warn personnel of any other potential form of terrorist attack.

(2) Measure 12. Keep all personnel involved in implementing antiterrorist contingency plans on call.

(3) Measure 13. Check plans for implementation of the next THREATCON.

(4) Measure 14. Move cars and objects (e.g., crates, trash containers) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.

(5) Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

(6) Measure 16. At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

(7) Measure 17. Examine mail (above the regular examination process) for letter or parcel bombs.

(8) Measure 18. Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.

(9) Measure 19. Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense, and to build confidence among staff and dependents.

(10) Measure 20. Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

(11) Measure 21. At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

(12) Measure 22. Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers. Identify the visitor's destination. Ensure that proper dignity is maintained, and if possible, ensure that female visitors are inspected only by a female qualified to conduct physical inspections.

(13) Measure 23. Operate random patrols to check vehicles, people, and buildings.

(14) Measure 24. Protect off-base military personnel and military vehicles in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or exiting the vehicle.

(15) Measure 25. Implement additional security measures for high-risk personnel as appropriate.

(16) Measure 26. Brief personnel who may augment guard forces on the use of deadly force. Ensure that there is no misunderstanding of these instructions.

(17) Measures 27. As appropriate, consult local authorities on the threat and mutual antiterrorism measures.

(18) Measures 28 and 29. To be determined.

d. THREATCON CHARLIE applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent. Implementation of measures in this THREATCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

(1) Measure 30. Continue, or introduce, all measures listed in THREATCON BRAVO.

(2) Measure 31. Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

(3) Measure 32. Limit access points to the absolute minimum.

(4) Measure 33. Strictly enforce control of entry. Randomly search vehicles.

(5) Measure 34. Enforce centralized parking of vehicles away from sensitive buildings.

(6) Measure 35. Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

(7) Measure 36. Increase patrolling of the installation.

(8) Measure 37. Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.

(9) Measure 38. Erect barriers and obstacles to control traffic flow.

(10) Measure 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to attacks.

(11) Measure 40. To be determined.

e. THREATCON DELTA applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is likely. Normally, this THREATCON is declared as a localized condition.

(1) Measure 41. Continue, or introduce, all measures listed for THREATCONs BRAVO and CHARLIE.

(2) Measure 42. Augment guards as necessary.

(3) Measure 43. Identify all vehicles within operational or mission-support areas.

(4) Measure 44. Search all vehicles and their contents before allowing entrance to the installation.

(5) Measure 45. Control access and implement positive identification of all personnel--no exceptions.

(6) Measure 46. Search all suitcases, briefcases, packages; etc., brought into the installation.

(7) Measure 47. Control access to all areas under the jurisdiction of the United States.

(8) Measure 48. Make frequent checks of the exterior of buildings and of parking areas.

(9) Measure 49. Minimize all administrative journeys and visits.

(10) Measure 50. Coordinate the possible closing of public and military roads and facilities with local authorities.

(11) Measure 51. To be determined.

SECTION II. SHIPBOARD TERRORIST THREAT CONDITIONS

2. Shipboard Terrorist THREATCON Measures. The measures outlined below are for use aboard vessels and serve two purposes. First, the crew is alerted, additional watches are created, and there is greater security. Second, these measures display the ship's resolve to prepare for and counter the terrorist threat. These actions will convey to anyone observing the ship's activities that the ship is prepared, the ship is an undesirable target, and the terrorist(s) should look elsewhere for a vulnerable target. The measures outlined below do not account for local conditions and regulations or current threat intelligence. The ship's command must maintain flexibility. As threat conditions change, the ship's crew must be prepared to take actions to counter the threat. When necessary, additional measures must be taken immediately. The simple solution to THREATCON CHARLIE or DELTA is to get under way, but this option may not always be available.

a. THREATCON ALPHA is declared when a general threat of possible terrorist activity is directed toward installations, vessels, and personnel, the nature and extent of which are unpredictable, and where circumstances do not justify full implementation of THREATCON BRAVO measures. However, it may be necessary to

implement certain selected measures from THREATCON BRAVO as a result of intelligence received or as a deterrent. The measures in this threat condition must be capable of being maintained indefinitely.

(1) Measure 1. Brief crew on the threat, ship security, and security precautions to be taken while ashore.

(2) Measure 2. Muster and brief security personnel on the threat and rules of engagement.

(3) Measure 3. Review security plans and keep them available. Keep on call key personnel who may be needed to implement security measures.

(4) Measure 4. Consistent with local rules, regulations, and status of forces agreement, post qualified armed fantail sentry and forecastle sentry. Rifles are the preferred weapon.

(5) Measure 5. Consistent with local rules, regulations, and SOFA, post qualified armed pier sentry and pier entrance sentry.

(6) Measure 6. Issue two-way radios to all sentries, roving patrols, quarterdeck watch, and response force. If practical, all guards will be equipped with at least two systems of communication (e.g., two-way radio, telephone, whistle, or signal light).

(7) Measure 7. Issue night vision devices to selected posted security personnel.

(8) Measure 8. Coordinate pier and fleet landing security with collocated forces and local authorities. Identify anticipated needs for mutual support (security personnel, boats, and equipment) and define methods of activation and communication.

(9) Measure 9. Tighten shipboard and pier access control procedures. Positively identify all personnel entering pier and fleet landing area--no exceptions.

(10) Measure 10. Consistent with local rules, regulations, and SOFA, establish unloading zone(s) on the pier away from the ship.

(11) Measure 11. Deploy barriers to keep vehicles away from the ship. Barriers may be ship's vehicles, equipment, or items available locally.

(12) Measure 12. Post signs in local language(s) to explain visiting and loitering restrictions.

(13) Measure 13. Inspect all vehicles entering pier and check for unauthorized personnel, weapons, and/or explosives.

(14) Measure 14. Inspect all personnel, hand-carried items, and packages before they come aboard. Where possible, screening should be at the pier entrance or foot of brow.

(15) Measure 15. Direct departing and arriving liberty boats to make a security tour around the ship and give special attention to the waterline and hull. Boats must be identifiable night and day to ship's personnel.

(16) Measure 16. Water taxis, ferries, bum boats, and other harbor craft require special concern because they can serve as an ideal platform for terrorists. Unauthorized craft should be kept away from the ship; authorized craft should be carefully controlled, surveilled, and covered.

(17) Measure 17. Identify and inspect workboats.

(18) Measure 18. Secure spaces not in use.

(19) Measure 19. Regulate shipboard lighting to best meet the threat environment. Lighting should include illumination of the waterline.

(20) Measure 20. Rig hawsepipe covers and rat guards on all lines, cable, and hoses. Consider using an anchor collar.

(21) Measure 21. Raise accommodation ladders, stern gates, jacob ladders, etc., when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

(22) Measure 22. Conduct security drills to include bomb threat and repel boarders exercises.

(23) Measure 23. Review individual actions in THREATCON BRAVO for possible implementation.

(24) Measure 24. To be determined.

b. THREATCON BRAVO is declared when an increased and more predictable threat of terrorist activity exists. The measures in this THREATCON must be capable of being maintained for weeks without causing undue hardships, without affecting operational capability, and without aggravating relations with local authorities.

(1) Measure 25. Maintain appropriate THREATCON ALPHA measures.

(2) Measure 26. Review liberty policy in light of the threat and revise it as necessary to maintain the safety and security of the ship and crew.

(3) Measure 27. Conduct divisional quarters at foul weather parade to determine the status of on-board personnel and to disseminate information.

(4) Measure 28. Ensure that an up-to-date list of bilingual personnel for the area of operations is readily available. Ensure the warning tape in the pilot house and/or quarterdeck that warns small craft to remain clear is in both the local language and English.

(5) Measure 29. Remind all personnel to: (a) be suspicious and inquisitive of strangers, particularly those carrying suitcases or other containers; (b) be alert for abandoned parcels or suitcases; (c) be alert for unattended vehicles in the vicinity; (d) be wary of any unusual activities; and (e) notify the duty officer of anything suspicious.

(6) Measure 30. Remind personnel to lock their parked vehicles and to carefully check them before entering.

(7) Measure 31. Designate and brief picket boat crews. Prepare boats and place crews on 15-minute alert. If the situation warrants, make random picket boat patrols in the immediate vicinity of the ship with the motor whaleboat or gig. Boat crews will be armed with M16 rifles, one M60 with 200 rounds of ammunition, and 10 concussion grenades.

(8) Measure 32. Consistent with local rules, regulations, and SOFA, establish armed brow watch on pier to check identification and inspect baggage before personnel board ship.

(9) Measure 33. Man signal bridge or pilot house and ensure flares are available to ward off approaching craft.

(10) Measure 34. After working hours, place armed sentries on a superstructure level from which they can best cover areas about the ship.

(11) Measure 35. Arm all members of the quarterdeck watch and SAT. In the absence of a SAT, arm two members of the SDF.

(12) Measure 36. Provide shotgun and ammunition to quarterdeck. If the situation warrants, place sentry with shotgun inside the superstructure at a site from which the quarterdeck can be covered.

(13) Measure 37. Issue arms to selected qualified officers to include Command Duty Officer (CDO) and Assistant Command Duty Officer (ACDO).

(14) Measure 38. Arm Sounding and Security Patrol.

(15) Measure 39. Muster and brief ammunition bearers or messengers.

(16) Measure 40. Implement procedures for expedient issue of firearms and ammunition from small arms locker (SAL). Ensure a set of SAL keys are readily available and in the possession of an officer designated for this duty by the commanding officer.

(17) Measure 41. Load additional small arms magazines to ensure adequate supply for security personnel and response forces.

(18) Measure 42. Inform local authorities of actions taken as the THREATCON increases.

(19) Measure 43. Test communications with local authorities and other US Navy ships in port.

(20) Measure 44. Instruct watches to conduct frequent random searches under piers, with emphasis on potential hiding places, pier pilings, and floating debris.

(21) Measure 45. Conduct searches of the ship's hull and boats at intermittent intervals and immediately before it puts to sea.

(22) Measure 46. Move cars and objects such as crates and trash containers 100 feet from the ship.

(23) Measure 47. Hoist boats aboard when not in use.

(24) Measure 48. Terminate all public visits.

(25) Measure 49. Set materiel condition YOKE, main deck and below.

(26) Measure 50. After working hours, reduce entry points to the ship's interior by securing selected entrances from the inside.

(27) Measure 51. Duty department heads ensure all spaces not in regular use are secured and inspected periodically.

(28) Measure 52. If two brows are rigged, remove one of them.

(29) Measure 53. Maintain capability to get under way on short notice or as specified by SOP. Consider

possible relocation sites (different pier, anchorage, etc.). Rig brow and accommodation ladder for immediate raising or removal.

(30) Measure 54. Ensure .50-caliber mount assemblies are in place with ammunition in ready service lockers (.50-caliber machineguns will be maintained in the armory, prefire checks completed, and ready for use).

(31) Measure 55. Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultralight aircraft.

(32) Measure 56. Obstruct possible helicopter landing areas in such a manner as to prevent hostile helicopters from landing.

(33) Measure 57. Review riot and crowd control procedures, asylum-seeker procedures, and bomb threat procedures.

(34) Measure 58. Monitor local communications (e.g., ship-to-ship, TV, radio, police scanners).

(35) Measure 59. Implement additional security measures for high-risk personnel as appropriate.

(36) Measure 60. Review individual actions in THREATCON CHARLIE for possible implementation.

(37) Measures 61 and 62. To be determined.

c. THREATCON CHARLIE is declared when an incident occurs or intelligence is received indicating that some form of terrorist action against installations, vessels, or personnel is imminent. Implementation of this THREATCON for more than a short period will probably create hardship and will affect the peacetime activities of the ship and its personnel.

(1) Measure 63. Maintain appropriate measures for THREATCONs ALPHA and BRAVO.

(2) Measure 64. Cancel liberty. Execute emergency recall.

(3) Measure 65. Be prepared to get under way on one 1 hour's notice or less. If conditions warrant, request permission to sortie.

(4) Measure 66. Muster and arm SAT, BAF, and reserve force (RF). Position SAT and BAF at designated location(s). Deploy RF to protect command structure and augment posted security watches.

(5) Measure 67. Place armed sentries on a superstructure level from which they can best cover areas about the ship.

(6) Measure 68. Establish .50- or .30-caliber machinegun positions.

(7) Measure 69. If available, deploy STINGER surface-to-air missiles IAW established ROE.

(8) Measure 70. Energize radar and establish watch.

(9) Measure 71. Ships with high-power sonars operate actively for random periods to deter underwater activity. Man passive sonar capable of detecting boats, swimmers, or underwater vehicles. Position any non-sonar-equipped ships within the acoustic envelope of sonar-equipped ships.

(10) Measure 72. Man one or more repair lockers. Establish communications with an extra watch in DC Central.

(11) Measure 73. Deploy picket boat. Boats should be identifiable night and day from the ship (e.g., by lights or flags).

(12) Measure 74. If feasible, deploy a helicopter as an observation or gun platform. The helicopter should be identifiable night and day from the ship.

(13) Measure 75. Activate antiswimmer watch. (Portions of watch may already be implemented by previous THREATCON measures).

(14) Measure 76. Issue weapons to selected officers and chief petty officers in the duty section (i.e., the commanding officer, executive officer, department heads).

(15) Measure 77. Issue concussion grenades to topside rovers, forecastle and fantail sentries, and bridge watch.

(16) Measure 78. Erect barriers and obstacles as required to control traffic flow.

(17) Measure 79. Strictly enforce entry control procedures and searches--no exceptions.

(18) Measure 80. Enforce boat exclusion zone.

(19) Measure 81. Minimize all off-ship administrative trips.

(20) Measure 82. Discontinue contract work.

(21) Measure 83. Set materiel condition ZEBRA, second deck and below.

(22) Measure 84. Secure from the inside all unguarded entry points to the interior of the ship.

(23) Measure 85. Rotate screws and cycle rudder(s) at frequent and irregular intervals.

(24) Measure 86. Rig additional firehoses. Charge the firehoses when manned just prior to actual use.

(25) Measure 87. Review individual actions in THREATCON DELTA for implementation.

(26) Measure 88. To be determined.

d. THREATCON DELTA is declared when a terrorist attack has occurred in the immediate area or intelligence has been received that indicates a terrorist action against a specific location or person is likely. Normally, this THREATCON is declared as a localized warning.

(1) Measure 89. Maintain appropriate THREATCONs ALPHA, BRAVO, and CHARLIE measures.

(2) Measure 90. Permit only necessary personnel topside.

(3) Measure 91. Prepare to get under way and, if possible, cancel port visit and depart.

(4) Measure 92. Post sentries with M60 machinegun(s) to cover possible helicopter landing areas.

(5) Measure 93. Arm selected personnel of the SDF.

(6) Measure 94. Deploy M-79 grenade launchers to cover approaches to ship.

(7) Measure 95. To be determined.

SECTION III. AVIATION FACILITY THREATCON PROCEDURES

3. General. In addition to basic THREATCON procedures, a variety of other tasks may need to be performed at aviation facilities. This is particularly true for airbases located in areas where the threat of terrorist attacks is high.

a. THREATCONs ALPHA AND BRAVO

(1) Planning

(a) Review THREATCONs ALPHA and BRAVO measures.

(b) Update THREATCONs ALPHA and BRAVO measures as required.

(2) Briefing and Liaison

(a) Brief all personnel on the threat, especially pilots, ground support crews, and air traffic controllers.

(b) Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations.

(c) Ensure duty officers are always available by telephone.

(d) Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.

(e) Be prepared to receive and direct aircraft from other stations.

(3) Precautions Inside the Perimeter

(a) Perform thorough and regular inspection of areas within the perimeters from which attacks on aircraft can be made.

(b) Take action to ensure no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.

(c) Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area--no exceptions.

(d) Search all vehicles, briefcases, packages, etc., entering the area.

(e) Erect barriers around potential targets if at all possible.

(f) Maintain firefighting equipment and conduct practice drills.

(g) Hold practice alerts within the perimeter.

(4) Precautions Outside the Perimeter

(a) Conduct, with local police, regular inspections of the perimeter--especially the area adjacent to flight paths.

(b) Advise the local police of any areas outside the perimeter where attacks could be mounted and that cannot be avoided by aircraft on takeoff or landing.

(c) Advise aircrews to report any unusual activity near approach and overshoot areas.

b. THREATCON CHARLIE

(1) Planning

(a) Review THREATCON CHARLIE measures.

(b) Update THREATCON CHARLIE measures as required.

(2) Briefing and Liaison

(a) Brief all personnel on the increased threat.

(b) Inform local police of increased threat.

(c) Coordinate with the local police on any precautionary measures taken outside the airfield's perimeters.

(d) Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.

(3) Precautions Inside the Perimeter

(a) Inspect all vehicles and buildings on a regular basis.

(b) Detail additional guards to be on call at short notice and consider augmenting firefighting details.

(c) Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.

(d) Reduce flying to essential operational flights only. Cease circuit flying if appropriate.

(e) Escort all visitors.

(f) Close relief landing grounds where appropriate.

(g) Check airfield diversion state.

(4) Precautions Outside the Perimeter

(a) Be prepared to react to requests for assistance.

(b) Provide troops to assist local police in searching for terrorists on approaches outside the perimeter of military airfields.

c. THREATCON DELTA

(1) Planning

(a) Review THREATCON DELTA measures.

(b) Update THREATCON DELTA measures as required.

(2) Briefings and Liaison

(a) Brief all personnel on the very high levels of threat.

(b) Inform local police of the increased threat.

(3) Precautions Inside the Perimeter

(a) Cease all flying except for specifically authorized operational sorties.

(b) Implement, if necessary, appropriate flying countermeasures.

(c) Be prepared to accept aircraft diverted from other stations.

(d) Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.

(4) Precautions Outside the Perimeter. Close military roads allowing access to the airbase.

JP 3-55

Reconnaissance, Surveillance, and Target Acq Sppt for Joint Op

TABLE OF CONTENTS

Inside Front Cover

Memorandum

Record of Changes

Preface

CHAPTER I... RSTA MISSION AREAS AND TASKS

- Overview
- RSTA Mission Areas
- Operations Security (OPSEC)
- Operational Deception (OPDEC)

CHAPTER II... REQUIRED JOINT RSTA CAPABILITIES

- Overview
- Types of Information
- Collection Capabilities and Limitations
- Required Capabilities

CHAPTER III... OPERATIONS

- Overview
- The Intelligence Cycle
- Command Relationships
- Planning RSTA Operations
- Tasking RSTA Operations
- RSTA Coordination
- RSTA Execution

CHAPTER IV... TARGETING

- Overview
- Targeting Objectives
- The Target
- Target Development
- Weaponeering Assessment
- Force Application Planning
- Execution Planning

Battle Damage Assessment
Mission Cycle
Coordination

APPENDIX A... References

APPENDIX B... Users Evaluation Report

Glossary

Part I--Acronyms and Abbreviations
Part II--Terms and Definitions

12-26-1996, 10:35:49

JP 3-55.1

JTTP for Unmanned Aerial Vehicles

TABLE OF CONTENTS

Inside Front Cover

Memorandum

Record of Changes

Preface

Chapter I... OVERVIEW

- General
- UAV Class Categories

Chapter II... EMPLOYMENT

- Mission
- Intelligence Requirements, Exploitation, and Dissemination
- Command and Control, Tasking, and Communications
- Airspace Control
- Planning
- Conduct of the Mission
- UAV System Advantages and Disadvantages
- Close-Range Unmanned Aerial Vehicle
- Short-Range Unmanned Aerial Vehicle

Appendix A... References

Appendix B... Users Evaluation Report

Glossary

- Part I--Abbreviations and Acronyms
- Part II--Terms and Definitions

Figure II-1... UAV System Setup with Control Stations Collocated
Figure II-2... UAV System Setup with Control Stations at Supported Unit
Figure II-3... UAV Airspace Control Measures (Overhead View)
Figure II-4... UAV Airspace Control Measures (Horizontal View)

Figure II-5... US Marine Corps CR-UAV
Figure II-6... US Army Augmented System
Figure II-7... SR-UAV System Description

Joint Pub 3-56.1
14 Nov 1994

JP 3-56.1

Command and Control for Joint Air Operations

Table of Contents

Preface

Executive Summary

CHAPTER I... Introduction

- Scope
- Joint Air Operations
- Organizing Joint Forces
- Military Operations Other Than War (MOOTW)
- Summary

CHAPTER II... General Considerations for Command and Control of Joint Air Operations

- Air Effort Available for Joint Air Operations
- Designation of a JFACC
- JFACC Authority and Command Relationships
- JFACC Responsibilities
- Airspace Control Considerations and the JFACC/ACA/AADC Relationship
- JFACC Organization
- Component Liaison
- JFACC Staff
- JFACC Assignments and Transition
- JFC Staff Option in Joint Air Operations
- JFC Staff Authority and Responsibilities
- JFC Staff Organization and Manning
- Transition Between JFC Staff and JFACC

CHAPTER III... Planning for Joint Air operations

- Concept of Joint Air Operations Development
- Joint Air Operations Plan
- Joint Air Operations Planning Process

CHAPTER IV... Targeting and Tasking for Joint Air Operations

Targeting
Targeting Process
Targeting Responsibilities
The Joint Air Tasking Cycle
Joint ATO Phases
Command, Control, Communications, Computers, and Intelligence (C4I)

Appendix A... Joint Air Operations Plan Format

Appendix B... Liaison Elements Within the JAOC

Appendix C... Joint Air Operations Center (JAOC) Divisions/Branches Descriptions

Appendix D... References

Appendix E... Administrative Instructions

Glossary

Part 1... Abbreviations and Acronyms

Part 2... Terms and Definitions

FIGURE

II-1... JFACC Responsibilities
II-2... Airspace Control Procedures Characteristics
II-3... Methods of Airspace Control
II-4... Notional JFACC Organization
II-5... JFACC Transition Considerations
III-1... Concept of Joint Air Operations Development
III-2... Joint Air Operations Planning Process
IV-1... Targeting Cycle Phases
IV-2... JFACC/JFC Staff Targeting Responsibilities
IV-3... Notional Air Tasking Cycle
IV-4... Notional 48 Hour Joint ATO Timeline

Source document in MS Word: here. NOTE: This document is no longer current. It has been superseded by the DoD Joint Security Implementation Guide (DJSIG).

Joint DoDIIS/Cryptologic SCI Information Systems Security Standards

31 March 2001

Revision 2

This Page Intentionally Blank

EXECUTIVE SUMMARY

(U) The policy of the U.S. Government is that all classified information must be appropriately safeguarded to assure the confidentiality, integrity, and availability of that information. This document provides procedural guidance for the protection, use, management, and dissemination of Sensitive Compartmented Information (SCI), and is applicable to the Department of Defense (DoD) to include DoD components and Government contractors who process SCI. The combination of security safeguards and procedures used for Information Systems (IS) shall assure compliance with DCID 6/3, NSA/CSS Manual 130-1 and DIAM 50-4. The JDCSISSS is a technical supplement to both the NSA/CSS Manual 130-1 and DIAM 50-4.

(U) The prime purpose of this document is to provide IS security implementation guidance relative to the management of SCI and the automated infrastructure used to process this information at the organizational level.

(U) Nothing in this document shall be construed to countermand or waive provisions of any Executive Order, National Policy, Department of Defense (DoD) Directive, or other provisions of regulatory policies or laws which are beyond the scope of authority of the Directors of the Defense Intelligence Agency (DIA) and the National Security Agency/Central Security Service (NSA/CSS).

TABLE OF CONTENTS

Paragraph

Executive Summary -

Chapter 1--General Information

BACKGROUND 1.1
POLICY 1.2
SCOPE AND APPLICABILITY 1.3
REFERENCES, ACRONYMS, AND DEFINITIONS 1.4
ROLES AND RESPONSIBILITIES 1.5
Principal Accrediting Authority (PAA) 1.5.1
Data Owner 1.5.2
Designated Approving Authority (DAA) 1.5.3
DAA Representative (Rep)/Service Certifying Organization (SCO) 1.5.4
NSA/CSS Senior Information Systems Security Program Manager (SISSPM) 1.5.5
Service Cryptologic Element (SCE) Information Systems Security Program Manager (ISSPM) 1.5.6
Commander/Commanding Officer Responsibility 1.5.7
Information Systems Security Manager (ISSM) 1.5.8
Information Systems Security Officer (ISSO) 1.5.9
Program Management Office (PMO)/Program manager (PM) 1.5.10
Privileged Users (e.g., System Administrator (SA)) 1.5.11
General Users 1.5.12
Prohibited Activities 1.5.13
CONFIGURATION CONTROL BOARD (CCB) OVERSIGHT 1.6
OTHER DOCUMENTATION SUPERSESSION 1.7

Chapter 2--Life Cycle Security

PURPOSE 2.1
SCOPE 2.2
PROCEDURES 2.3
Concepts Development Phase 2.3.1
IS Security Design 2.3.1.1
Statement of Work (SOW) Requirements 2.3.1.2
Additional Documentation 2.3.1.3
Design Phase 2.3.2
Levels-of-Concern 2.3.2.1
Protection Levels 2.3.2.2
Development Phase 2.3.3
Test, Certification and Accreditation Phase 2.3.4
Time Line for Certification Activities 2.3.4.1
Deployment and Operations Phase 2.3.5
Recertification Phase 2.3.6
Disposal Phase 2.3.7

Chapter 3--Signals Intelligence (SIGINT) Systems Accreditation Process and Procedures

PURPOSE 3.1
SCOPE 3.2
DISCUSSION 3.3
Accreditation 3.3.1
Configuration Management 3.3.2
ACCREDITATION IN GENERAL 3.4
Formal Accreditation 3.4.1
Issuing Accreditation 3.4.2
Reaccreditation 3.4.3
Rescinding Accreditation 3.4.4
Accreditation 3-Year Anniversary Review 3.4.5
Authorized Exemptions From Accreditation 3.4.6
IS Approval-To-Operate 3.4.7
TEMPEST 3.4.8
ACCREDITATION PROCEDURES 3.5
Accreditation Requests 3.5.1
Accreditation Requests Initiated at the Unit Level 3.5.1.1
Accreditation Initiated Through Downward-Directed Programs 3.5.1.2
Accreditation at a Single-Service Site Including the Regional SIGINT Operation Centers 3.5.1.3
Accreditation at a Multi-Service Site 3.5.1.4
Operational Systems Under Control of the Commander/Commanding Officer 3.5.1.4.1
SCE Unique Systems Not Directly Supporting The Primary Mission 3.5.1.4.2
Assignment of a HSO at a Multi-Service Site 3.5.1.4.3
Accreditation by SCE Tenants Located at Non-SCE Interservice or Intercommand Sites 3.5.1.5
Submitting The System Security Plan (SSP) 3.5.2
Single Accreditation 3.5.2.1
Type Accreditation 3.5.2.2
Format and Content 3.5.2.3
SSP and Database Classification 3.5.3
Database Classification 3.5.3.1
SSP Classification 3.5.3.2

Chapter 4--Department of Defense Intelligence Information Systems (DoDIIS) Site-Based Accreditation

PURPOSE 4.1
SCOPE 4.2
SYSTEM CERTIFICATION AND ACCREDITATION PROCEDURES 4.3
System Certification and Accreditation Compliance 4.3.1
The System Certification and Accreditation Process 4.3.2
Phase 1 ..... 4.3.2.1
Phase 2 ..... 4.3.2.2
Phase 3 ..... 4.3.2.3
Phase 4 ..... 4.3.2.4
SITE-BASED ACCREDITATION METHODOLOGY 4.4
Site-Based Accreditation Methodology Compliance 4.4.1
The Site-Based Accreditation Process 4.4.2
(Site Initial Visit) Initial Site Certification Visit 4.4.2.1
(Site Evaluation Visit) Site Security and Engineering Certification Testing and Evaluation and Site Accreditation 4.4.2.2
(Site Compliance Visit) Vulnerability Assessment and Compliance Verification 4.4.2.3
CONTRACTOR ACCREDITATION 4.5
ACCREDITATION REVIEW 4.6
MINIMUM SECURITY REQUIREMENTS 4.7

Chapter 5--TEMPEST

PURPOSE..... 5.1
SCOPE..... 5.2
DEFINITIONS..... 5.3
TEMPEST COMPLIANCE..... 5.4
ACCREDITATION..... 5.5
TEMPEST Countermeasures Review..... 5.5.1
General Documentation..... 5.5.2
TEMPEST/ISD Accreditation..... 5.5.3
Installation Requirements..... 5.6

Chapter 6--Security Requirements for Users

PURPOSE..... 6.1
SCOPE..... 6.2
MINUMUM SECURITY REQUIREMENTS..... 6.3
Identification and Authentication Requirements..... 6.3.1
Password Requirements..... 6.3.2
IS Warning Banner..... 6.3.3
Configuration Requirements..... 6.3.4
Malicious Code Detection..... 6.3.5
Virus Scanning Requirements..... 6.3.6
Information Storage Media..... 6.3.7
Label Placement..... 6.3.7.1
Data Descriptor Label..... 6.3.7.2
Classification Markings..... 6.3.7.3
Control and Accounting of Media..... 6.3.7.4
Information Storage Media Control..... 6.3.7.4.1
Inspections..... 6.3.7.4.2
Control Procedures..... 6.3.7.4.3
Other Categories of Storage Media..... 6.3.7.4.4
Hardware Labeling Requirements..... 6.3.8
Security Training Requirements..... 6.3.9
Security Awareness and Training Program..... 6.3.9.1
Awareness Level..... 6.3.9.1.1
Performance Level..... 6.3.9.1.2
Destruction of Media..... 6.3.10
Information Transfer and Accounting Procedures..... 6.3.11

Chapter 7--Security Guidelines for the Privileged User and General User (GU)

PURPOSE..... 7.1
SCOPE..... 7.2
SECURITY TRAINING..... 7.3
General Users Training..... 7.3.1
Privileged Users Training..... 7.3.2
Security Awareness Training Program..... 7.3.3
Awareness Level..... 7.3.3.1
Performance Level..... 7.3.3.2
PROCEDURES..... 7.4
Identification and Authentication Requirements..... 7.4.1
Documenting USERIDs and Passwords..... 7.4.1.1
USERID and Password Issuing Authority and Accountability..... 7.4.1.2
Supervisor Authorization..... 7.4.1.3
Access Requirements Validation..... 7.4.1.4
Control Guidelines..... 7.4.2
System Access Removal Procedures..... 7.4.3
Audit Trail Requirements..... 7.4.4
Automated Audit Trail Information Requirements..... 7.4.4.1
Manual Audit Trail Implementation..... 7.4.4.2
Products of Audit Trail Information..... 7.4.4.3
Audit Trail Checks and Reviews..... 7.4.4.4
Audit Trail Records Retention..... 7.4.4.5
Automatic Logout Requirements..... 7.4.5
Limited Access Attempts..... 7.4.6
Use of Windows Screen Locks..... 7.4.7
Testing, Straining, and Hacking..... 7.4.8
Warning Banners..... 7.4.9
Network Monitoring..... 7.4.10
Maintenance Monitoring..... 7.4.10.1
Targeted Monitoring..... 7.4.10.2

Chapter 8--Information Systems (IS) Incident Reporting

PURPOSE..... 8.1
SCOPE..... 8.2
PROCEDURES..... 8.3
Reporting Decision..... 8.3.1
Types of IS Incidents and Reports..... 8.3.2
Reporting Incidents..... 8.3.3
Report Format and Content..... 8.3.4
Follow-On Action..... 8.3.5

Chapter 9--Information System (IS) Monitoring Activities

PURPOSE..... 9.1
SCOPE..... 9.2
PROCEDURES..... 9.3
IS Warning Banner..... 9.3.1
Warning Labels..... 9.3.2
Action To Be Taken In A Monitoring Incident..... 9.3.3
Review System Specific Security Features..... 9.3.4

Chapter 10--Malicious Code Prevention

PURPOSE..... 10.1
SCOPE..... 10.2
DEFINITIONS..... 10.3
Malicious Code..... 10.3.1
Mobile Code..... 10.3.2
Malicious Mobile Code..... 10.3.3
Mobile Code Technologies..... 10.3.4
Trusted Source..... 10.3.5
Screening..... 10.3.6
PROCEDURES..... 10.4
Preventive Procedures..... 10.4.1
Malicious Code Detection..... 10.4.2
MALICIOUS CODE SECURITY REQUIREMENTS..... 10.5
Prevention Steps to be Taken..... 10.5.1

Chapter 11--Software

PURPOSE..... 11.1
SCOPE..... 11.2
PROCEDURES..... 11.3
LOW RISK SOFTWARE..... 11.4
HIGH RISK SOFTWARE..... 11.5
Public Domain Software..... 11.5.1

Unauthorized Software..... 11.5.2
EMBEDDED SOFTWARE..... 11.6
POLICY EXCEPTIONS..... 11.7

Chapter 12--Information Storage Media Control and Accounting Procedures

PURPOSE..... 12.1
SCOPE..... 12.2
PROCEDURES..... 12.3
Information Storage Media Control..... 12.3.1
Inspections..... 12.3.1.1
Control Procedures..... 12.3.1.2
Other Categories of Storage Media..... 12.3.1.3
Audits and Reports..... 12.3.2
Destruction of Media..... 12.3.3

Chapter 13-- Information Storage Media Labeling and Product Marking Requirements

PURPOSE..... 13.1
SCOPE..... 13.2
PROCEDURES..... 13.3
Information Storage Media..... 13.3.1
Label Placement..... 13.3.1.1
Data Descriptor Label..... 13.3.1.2
Classification Markings..... 13.3.2

Chapter 14--Information Systems (IS) Maintenance Procedures

PURPOSE..... 14.1
SCOPE..... 14.2
PROCEDURES..... 14.3
Maintenance Personnel..... 14.3.1
Maintenance by Cleared Personnel..... 14.3.1.1
Maintenance by Uncleared (or Lower-Cleared) Personnel..... 14.3.1.2
General Maintenance Requirements..... 14.3.2
Maintenance Log..... 14.3.2.1
Location of Maintenance..... 14.3.2.2
Removal of Systems/Components..... 14.3.2.3
Use of Network Analyzers..... 14.3.2.4
Use of Diagnostics..... 14.3.2.5
Introduction of Maintenance Equipment Into a Sensitive Compartmented Information Facility (SCIF)..... 14.3.2.6
Maintenance and System Security..... 14.3.3
Remote Maintenance..... 14.3.4
Maintenance Performed With The Same Level of Security..... 14.3.4.1
Maintenance Performed With a Different Level of Security..... 14.3.4.2
Initiating and Terminating Remote Access..... 14.3.4.3
Keystroke Monitoring Requirements..... 14.3.4.4
Other Requirements/Considerations..... 14.3.4.5
Life Cycle Maintenance..... 14.3.5

Chapter 15--Portable Electronic Devices

PURPOSE..... 15.1
SCOPE..... 15.2
PROCEDURES..... 15.3
Approval Requirements..... 15.3.1
Handling Procedures..... 15.3.2
Standard Operating Procedure (SOP) Development..... 15.3.2.1
Classified Processing..... 15.3.2.2
Standard Operating Procedures (SOP) Approval..... 15.3.3

Chapter 16—Security Procedures for Information Systems (IS) and Facsimile (FAX) use of the Public Telephone Network

PURPOSE..... 16.1
SCOPE..... 16.2
PROCEDURES..... 16.3
DAA Rep/SCO Validation and Approval..... 16.3.1
UNCLASSIFIED CONNECTIVITY..... 16.4
Unclassified Facsimile Guidelines..... 16.4.1
Unclassified Facsimile Approval..... 16.4.1.1
Request for Unclassified Fax Approval..... 16.4.1.1.1
Physical Disconnect of Unclassified Fax Equipment..... 16.4.1.2
Fax Header Information..... 16.4.1.3
Unclassified Computer FAX/modem - telephone guidelines..... 16.4.2
Unclassified Computer FAX/modem accreditation support..... 16.4.2.1
Physical Disconnect of Unclassified Computer Fax/Modem equipment..... 16.4.2.2
Fax/Modem header Information..... 16.4.2.3
Data Retrieval..... 16.4.2.4
Importation of High Risk software..... 16.4.2.5
Publicly Accessible Unclassified Open Source Information Systems..... 16.4.3
Open Source Information Systems Connectivity 16.4.3.1
CLASSIFIED CONNECTIVITY..... 16.5
Secure Telephone Unit (STU)-III/Data Port Security Procedures..... 16.5.1
Identification and Authentication..... 16.5.2
Use of the Defense Switching Network (DSN) with a STU-III..... 16.5.3
STU-III Data Port/Fax Connectivity..... 16.5.4
Request for STU-III/Fax Connectivity..... 16.5.4.1
STU-III Fax Audit Logs..... 16.5.4.2
STU-III Connectivity Restrictions..... 16.5.4.3
STU-III Data Port Connectivity within a SCIF..... 16.5.5
Connectivity Requirements..... 16.5.5.1
STU-III Data Port Audit Logs..... 16.5.5.1.1
Connectivity Restrictions..... 16.5.5.1.2

Chapter 17-Interconnecting Information Systems

PURPOSE..... 17.1
SCOPE..... 17.2
DISCUSSION..... 17.3
Interconnected Information Systems..... 17.3.1
Inter-Domain Connections..... 17.3.2
Controlled Interface..... 17.3.3
One-Way Connections..... 17.3.3.1
Equal Classification Connection..... 17.3.3.1.1
Low to High Connections..... 17.3.3.1.2
High to Low Connections..... 17.3.3.1.3
Other Unequal Classification Level Connections..... 17.3.3.1.4
Dual-Direction Connections..... 17.3.3.2
Multi-Domain Connections..... 17.3.3.3
Review Procedures..... 17.3.4
Reliable Human Review..... 17.3.4.1
Automated Review..... 17.3.4.2

Chapter 18-Information Transfer and Accounting Procedures

PURPOSE..... 18.1
SCOPE..... 18.2
PROCEDURES..... 18.3
Reliable Human Review of Data..... 18.3.1

Media Transfers In/Out of an Organization..... 18.3.2
Disposition of Excess or Obsolete COTS Software..... 18.3.3
High to Low Data Transfers by Media..... 18.3.4
PL-3 and Below Functionality..... 18.3.4.1
PL-4 and Above Functionality..... 18.3.4.2
Low to High Data Transfers by Media..... 18.3.5
Demonstration Software..... 18.3.6

Chapter 19--Multi-Position Switches

PURPOSE..... 19.1
SCOPE..... 19.2
POLICY..... 19.3
RESPONSIBILITIES..... 19.4
DAA Rep..... 19.4.1
ISSM..... 19.4.2
ISSO/System Administrator..... 19.4.3
AIS Requirements..... 19.5
Labels..... 19.5.1
Desktop Backgrounds..... 19.5.2
Screenlocks..... 19.5.3
Smart Keys/Permanent Storage Medium..... 19.5.4
Hot Key Capability..... 19.5.5
Scanning Capability..... 19.5.6
Wireless or Infrared Technology..... 19.5.7
Unique Password Requirement..... 19.5.8
Data Hierarchy..... 19.5.9
Security CONOPS..... 19.5.10
Training..... 19.5.11
TEMPEST..... 19.5.12
Procedures for LOGON/Switching Between Systems..... 19.5.13
KVM SWITCH USER AGREEMENT..... 19.6

Chapter 20--Clearing, Sanitizing, and Releasing Computer Components

PURPOSE..... 20.1
SCOPE..... 20.2
RESPONSIBILITIES..... 20.3
PROCEDURES..... 20.4
Review of Terms..... 20.4.1
Clearing..... 20.4.1.1
Sanitizing (Also Purging)..... 20.4.1.2
Destruction..... 20.4.1.3
Declassification..... 20.4.1.4
Periods Processing..... 20.4.1.5
Overwriting Media..... 20.4.2
Overwriting Procedure..... 20.4.2.1
Overwrite Verification..... 20.4.2.2
Degaussing Media..... 20.4.3
Magnetic Media Coercivity..... 20.4.3.1
Types of Degausser..... 20.4.3.2
Degausser Requirements..... 20.4.3.3
Use of a Degausser..... 20.4.3.4
Sanitizing Media..... 20.4.4
Destroying Media..... 20.4.5
Expendable Item Destruction..... 20.4.5.1
Destruction of Hard Disks and Disk Packs..... 20.4.5.2
Hard Disks..... 20.4.5.2.1
Shipping Instructions..... 20.4.5.2.2
Disk Packs..... 20.4.5.2.3
Optical Storage Media..... 20.4.5.2.4
Malfunctioning Media..... 20.4.6
Release of Memory Components and Boards..... 20.4.7
Volatile Memory Components..... 20.4.7.1
Nonvolatile Memory Components..... 20.4.7.2
Other Nonvolatile Media..... 20.4.7.3
Visual Displays..... 20.4.7.3.1
Printer Platens and Ribbons..... 20.4.7.3.2
Laser Printer Drums, Belts, and Cartridges..... 20.4.7.3.3
Clearing Systems for Periods Processing..... 20.4.8
Release of Systems and Components..... 20.4.9
Documenting IS Release or Disposal..... 20.4.9.1

Chapter 21--Other Security Requirements

PURPOSE..... 21.1
SCOPE..... 21.2
REQUIREMENTS..... 21.3
Contingency Planning..... 21.3.1
Backup..... 21.3.1.1
Responsibilities..... 21.3.1.2
Foreign National Access to Systems Processing Classified Information..... 21.3.2
Tactical/Deployable Systems..... 21.3.3
Resolving Conflicting Requirements..... 21.3.3.1
Specific Conflicting Requirements..... 21.3.3.2
Guest Systems in a SCIF..... 21.3.4
SCI Systems With Certification..... 21.3.4.1
SCI Systems Without Certification..... 21.3.4.2
Unclassified or Collateral Systems..... 21.3.4.3
Other Requirements..... 21.3.5

Chapter 22--Information Systems (IS) and Network Security Self-Inspection Aid

PURPOSE..... 22.1
SCOPE..... 22.2
APPLICABILITY..... 22.3
PROCEDURES..... 22.4

Figures **Page**

3.1 General Accreditation Review and Approval Cycle..... 14
3.2 Multi-Service Accreditation Flow..... 17
7.1 Sample NSA/CSS Form G6521..... 30
8.1 Sample Incident Report Message..... 36
9.1 Information System Warning Banner..... 38
9.2 Warning Label..... 38
19.1 KVM Switch User Agreement Form..... 65
20.1 Sample NSA/CSS Form G6522..... 72

Tables

9.1. Recommended Incident Response Actions..... 39
9.2. Sample Monitoring Investigation Questions..... 39
20.1. Sanitizing Data Storage Media..... 67
20.2. Sanitizing System Components..... 68

22.1. Is and Network Security Self-Inspection Checklist..... 78

Appendices

Appendix A--References..... A-1
Appendix B--Glossary of Acronyms, Abbreviations, and Terms..... B-1
Appendix C--Summary of Revisions..... C-1

CHAPTER 1

GENERAL INFORMATION

1.1. (U) BACKGROUND. The DIA DoDIIS Information Assurance (IA) Program (Air Force, Army, and Navy Service Certification Organizations -- SCO -- and NIMA Certification Authority) and NSA/CSS Information Assurance (IA) Program (Air Force, Army, and Navy Service Cryptologic Elements - SCE) identified a requirement to standardize security procedures used in the management of Sensitive Compartmented Information (SCI) systems and the information they process. SCI is defined as information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products. These special community controls are formal systems of restricted access established to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs. It was also determined that by standardizing procedural guidelines, it would significantly improve support to the increasingly interconnected customer base of the Joint Services. This document describes the protection philosophy and functional procedures essential in the implementation of an effective Information Assurance (IA) Program. Further, it provides implementation guidelines and procedures applicable to the protection, use, management, and dissemination of SCI; assigns responsibilities; and establishes procedures for the development, management, and operations of systems and networks used for processing SCI. The primary purpose of this supplemental guidance is to address day-to-day IS security issues and provide support to those responsible for managing SCI and the automated infrastructure used to process this information at the organizational level.

1.2. (U) POLICY. U.S. Government policy requires all classified information be appropriately safeguarded to ensure the confidentiality, integrity, and availability of the information. Safeguards will be applied such that information is accessed only by authorized persons and processes, is used only for its authorized purpose, retains its content integrity, is available to satisfy mission requirements, and is marked and labeled as required. SCI created, stored, processed, or transmitted in or over Information Systems (ISs) covered by DCI policy and supplementing directives shall be properly managed and protected throughout all phases of a system's life cycle. The combination of security safeguards and procedures shall assure that the system and users are in compliance with DCID 6/3, NSA/CSS Manual 130-1, DIAM 50-4, and the JDCSISSS supplement to NSA/CSS Manual 130-1 and DIAM 50-4. This document shall not be construed to countermand or waive provisions of any Executive Order, National Policy, Department of Defense (DoD) Directive, or other provisions of regulatory policies or laws which are beyond the scope of authority of the Directors of the Defense Intelligence Agency (DIA) and the National Security Agency/Central Security Service (NSA/CSS). Any perceived contradictions with higher-level policy should be forwarded to the appropriate Designated Approving Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO) for resolution.

1.3. (U) SCOPE AND APPLICABILITY. This document contains procedures and identifies requirements that shall be applied to all systems processing Sensitive Compartmented Information (SCI) under the cognizance of the Department of Defense (DoD), to include: Office of the Secretary of Defense (OSD), the Chairman of the Joint Chiefs of Staff and the Joint Staff, the United and Joint Commands, the Defense Agencies and Field Activities, the Military Departments (including their National Guard and Reserve components), National Security Agency (NSA)/Central Security Service (CSS) and Service Cryptologic Elements, National Image and Mapping Agency (NIMA), the Inspector General of the DoD, and Government contractors supporting DoD who process SCI. This includes systems that are: airborne, mobile, afloat, in-garrison, tactical, mission, administrative, embedded, portable, Government purchased, Government leased, or on loan from other Government sources. Contained also within this document is a collective set of procedures and protection mechanisms for Information Systems (ISs) and networks used in SCI processing that must be enforced throughout all phases of the IS life-cycle, to include:

- Concept Development
- Design
- Development
- Deployment
- Operations
- Recertification
- Disposal

1.4. (U) REFERENCES, ACRONYMS, AND DEFINITIONS. Appendix A provides a comprehensive list of national, department, and agency publications that are used in conjunction with this document and augments these reference sources. The acronyms used in this document are contained in part 1 of Appendix B. The terminology extracted from various IS related documents are included as part 2 of Appendix B.

1.5. (U) ROLES AND RESPONSIBILITIES. The roles and responsibilities of the personnel involved with IS security are summarized in the paragraphs below. Personnel in the roles defined below must attend training and certification as directed by DoD and meet DCID 6/3 prerequisites.

1.5.1. (U) Principal Accrediting Authority (PAA). The PAA has ultimate security responsibility for his/her organization. This responsibility includes IA program oversight, development, and implementation. In general, much of this person's operational authority is delegated to DAAs. Responsibilities of the PAA shall include:

- Establishing a department or agency IA Security Program.
- Appointing DAAs.
- Approving or disapproving further delegation of the DAA's authority.
- Ensuring that the DAA is supported by individuals knowledgeable in all areas of security such that a technically correct assessment of the security characteristics of new ISs can be formalized.
- Ensuring the implementation of the requirements set forth in U.S. Government IS security policy.
- Ensuring accountability for the protection of the information under his/her purview.
- Ensuring availability of security education, training, and awareness, to ensure consistency and reciprocity.
- Establishing a joint compliance and oversight mechanism to validate the consistent implementation of IS security policy.
- Approving the operation of system(s) that do not meet the requirements specified in DoD and Intelligence Community (IC) IS security documents. However, such approval shall be in writing, and the PAA granting such approval shall also document, in writing, his/her responsibility for the resulting residual risk(s) and inform other PAAs responsible for systems interconnected to this system.
- Overseeing the management of new IS development and implementation.
- Ensuring that security is incorporated as an element of the IS life-cycle process.

1.5.2. (U) Data Owner. Responsibilities of the Data Owner shall include, but are not limited to:

- Providing guidance to the PAA/DAA concerning:
  - the sensitivity of information under the Data Owner's purview;
  - the PAA/DAA's decision regarding the Levels-of-Concern for confidentiality, integrity, and availability; and
  - specific requirements for managing the owner's data (e.g., incident response, information contamination to other systems/media, and unique audit requirements).
- Determining whether foreign nationals may access information systems accredited under this manual. Access must be consistent with DCID 1/7 and DCID 5/6.

1.5.3. (U) Designated Approving Authority (DAA). The DAA shall:

- Be a U.S. citizen;
- Be an employee of the United States Government; and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

Responsibilities of the DAA shall include, but are not limited to:

- Ensuring each system is properly accredited/certified based on system environment, sensitivity levels and security safeguards.
- Issuing written accreditation/certification statements.
- Ensuring records are maintained for all IS accreditations/certifications under his/her purview to include use of automated information assurance tools.
- Ensuring all of the appropriate roles and responsibilities outlined in this directive are accomplished for each IS.
- Ensuring that operational information systems security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority.
- Ensuring that a security education, training, and awareness program is in place.
- Ensuring that security is incorporated as an element of the life-cycle process.
- Ensuring that the DAA Representatives (Rep)/Service Certifying Organization (SCO) members are trained and certified to properly perform their responsibilities.
- Providing written notification to the cognizant PAA and Data Owner prior to granting any foreign national access to the system.
- Ensuring that organizations plan, budget, allocate, and spend adequate resources in support of IS security.
- Ensuring consideration and acknowledgement of Counter-Intelligence activities during the C&A process.
- Reporting security-related events to affected parties (i.e., interconnected systems), data owners, and all involved PAAs.

1.5.4. (U) DAA Representative (Rep)/Service Certifying Organization (SCO)

- The DAA Rep/SCO member shall be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

Responsibilities of the DAA Rep/SCO, under the direction of the DAA, shall include:

- Developing and overseeing operational information systems security implementation policy and guidelines.
- Ensuring that security testing and evaluation is completed and documented.
- Advising the DAA on the use of specific security mechanisms.
- Maintaining appropriate system accreditation documentation.
- Overseeing and periodically reviewing system security to accommodate possible changes that may have taken place.
- Advising the Information Systems Security Managers (ISSMs) and Information System Security Officers (ISSOs) concerning the levels of concern for confidentiality, integrity, and availability for the data on a system.
- Evaluating threats and vulnerabilities to ascertain the need for additional safeguards.
- Ensuring that a record is maintained of all security-related vulnerabilities and ensuring serious or unresolved violations are reported to the DAA.
- Ensuring that certification is accomplished for each IS.
- Evaluating certification documentation and providing written recommendations for accreditation to the DAA.
- Ensuring all ISSMs and ISSOs receive technical and security training to carry out their duties.
- Assessing changes in the system, its environment, and operational need that could affect the accreditation.

1.5.5. (U) NSA/CSS Senior Information Systems Security Program Manager (SISSPM)

- The SISSPM shall be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

The SISSPM responsibilities shall include but are not limited to the following:

- Developing metrics, measuring and reporting progress on improving ISS in operational systems and networks.
- Establishing and maintaining career development and training for ISS personnel under their purview.
- Serving as the operational representative to the NSA/CSS Information System Security Incident Board (NISSIB).
- Representing the operational ISS view to the Operational Information Systems Security Steering Group.
- Directing Field, SCE and regional ISSPMs in actions related to the NSA/CSS Operational IS Security Program.
- Assisting the NISIRT in managing ISS incidents and in implementing fixes to identified vulnerabilities in operational ISs.
- Promoting general operational information systems security awareness.
- Providing technical and policy guidance to ISS Security personnel.
- Providing a forum for information exchange on computer security issues with the Information Systems Security Managers.

1.5.6. (U) Service Cryptologic Element (SCE) Information Systems Security Program Manager (ISSPM).

- The SCE ISSPM shall be a U.S. citizen and

- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

The SCE ISSPM responsibilities include:

- Acting as liaison on matters concerning IS and Network security to the NSA/CSS Senior Information Systems Security Program Manager (SISSPM) and to the appropriate military headquarters.
- Ensuring the accreditation of all SCE ISs.
- Reviewing all certification/accreditation support documentation for proof of adequate IS and Network security procedures and, based upon the review, recommending approval or disapproval to the appropriate DAA.
- Forwarding reviewed certification/System Security Plan (SSP) for ISs to the NSA/CSS SISSPM, as required.
- Granting interim approval-to-operate and formal accreditation of ISs as authorized by NSA/CSS DAA.
- Reviewing requests to bypass, strain, or test security mechanisms, or conduct network monitoring or keystroke monitoring and obtaining approval/disapproval for SCI requests from the NSA/CSS SISSPM and approving/disapproving requests for unclassified and collateral systems.
- Ensuring life-cycle security integrity of all SCE ISs.
- Developing procedures necessary to implement higher level regulations and directives.
- Providing guidance and policy to all subordinate SCE organizations.
- Promoting the nomination of SCE personnel for NSA/CSS Security Achievement Awards.
- Managing the SCE IS and Network Security Training Program to include:
  - Ensuring all SCE ISSMs and ISSOs attend the National Cryptologic School ND-225 course, "Operational IS Security" or equivalent.
  - Coordinating the training of nominees with the National Cryptologic School.
  - Publishing SCE annual training schedules for the ND-225 course, which is published in October-November for the following calendar year.
  - Reporting name, organization, and address of all students to the National Cryptologic School for certificates of completion.
  - Developing unique SCE courses and materials for training, as necessary.
- Maintaining a level of expertise by attending IS and Network security conferences, symposiums, and training courses sponsored by other agencies.
- Augmenting SCE inspections, both Inspector General (IG) and others, upon request.
- Reviewing requirements for approving public-domain software before its use on any SCE IS.

1.5.7. (U) Commander/Commanding Officer (CO)/Senior Intelligence Officer (SIO) Responsibility. Commanders/CO/SIOs, in conjunction with their ISSM/ISSOs/System Administrators (SA), will work together to present a cohesive training program, both for users and IS & network security personnel. If well developed, and effectively implemented, the security program can help neutralize IS security threats, prevent the compromise or loss of classified information, and produce users who act effectively to secure system resources. The responsibilities of the Commander/CO/SIO include:

- Appointing an ISSM in writing and, where applicable, ensuring a copy of orders are forwarded to the SCE organization's ISSPM or the DIA DAA Rep/SCO.
- Ensuring the establishment and funding of an effective and responsive IS Security (ISS) Program.
- Participating as an active member of the organization's CCB or appoint a representative to act in his/her absence.
- Ensuring that users and ISS personnel receive DoD-mandated certification training IAW their responsibilities as part of an approved ISS training program.
- Ensuring ISS policies are enforced and implemented.

1.5.8. (U) Information Systems Security Manager (ISSM). The ISSM is appointed in writing by the authority at a site responsible for information system security. ISSM responsibilities should not be assigned as collateral duties, if at all possible. The ISSM shall:

- Be a U.S. citizen;
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system; and
- Attend ND-225 training or equivalent.

The ISSM responsibilities include:

- Forwarding a copy of his/her appointment letter to the DAA Rep/SCO.
- Developing and maintaining a formal IS security program.
- Implementing and enforcing IS security policies.
- Reviewing and endorsing all IS accreditation/certification support documentation packages.
- Overseeing all ISSOs to ensure they follow established IS policies and procedures.
- Ensuring ISSM/ISSO review weekly bulletins and advisories that impact security of site information systems to include, AFCERT, ACERT, NAVCIRT, IAVA, and DISA ASSIST bulletins.
- Ensuring that periodic testing (monthly for PL-5 systems) is conducted to evaluate the security posture of the ISs by employing various intrusion/attack detection and monitoring tools (shared responsibility with ISSOs).
- Ensuring that all ISSOs receive the necessary technical (e.g., operating system, networking, security management, SysAdmin) and security training (e.g., ND-225 or equivalent) to carry out their duties.
- Assisting ISSOs to ensure proper decisions are made concerning the levels of concern for confidentiality, integrity, and availability of the data, and the protection levels for confidentiality for the system.
- Ensuring the development of system accreditation/certification documentation by reviewing and endorsing such documentation and recommending action to the DAA Rep/SCO.
- Ensuring approved procedures are in place for clearing, purging, declassifying, and releasing system memory, media, and output.
- Maintaining, as required by the DAA Rep/SCO, a repository for all system accreditation/certification documentation and modifications.
- Coordinating IS security inspections, tests, and reviews.
- Investigating and reporting (to the DAA/DAA Rep/SCO and local management) security violations and incidents, as appropriate.
- Ensuring proper protection and corrective measures have been taken when an IS incident or vulnerability has been discovered.
- Ensuring data ownership and responsibilities are established for each IS, to include accountability, access and special handling requirements.
- Ensuring development and implementation of an effective IS security education, training, and awareness program.
- Ensuring development and implementation of procedures in accordance with configuration management (CM) policies and practices for authorizing the use of hardware/software on an IS. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM/ISSO and appropriate approving authority prior to the change.
- Developing procedures for responding to security incidents, and for investigating and reporting (to the DAA Rep/SCO and to local management) security violations and incidents, as appropriate.
- Serving as a member of the configuration management board, where one exists (however, the ISSM may elect to delegate this responsibility to the ISSO.)
- Working knowledge of system functions, security policies, technical security safeguards, and operational security measures.
- Accessing only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

1.5.9. (U) Information Systems Security Officer (ISSO). The ISSO shall:

- Be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

Responsibilities of the ISSO shall include:

- Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices as outlined in the accreditation/certification support documentation package.
- Attending required technical (e.g., operating system, networking, security management, SysAdmin) and security (e.g., ND-225 or equivalent) training relative to assigned duties.
- Ensuring all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS.
- Ensuring that proper decisions are made concerning levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality for the system.
- Reporting all security-related incidents to the ISSM.
- Initiating protective and corrective measures when a security incident or vulnerability is discovered, with the approval of the ISSM.
- Developing and maintaining an accreditation/certification support documentation package for system(s) for which they are responsible.
- Conducting periodic reviews to ensure compliance with the accreditation/certification support documentation package.
- Ensuring Configuration Management (CM) for IS software and hardware, to include IS warning banners, is maintained and documented.
- Serving as member of the Configuration Management Board if so designated by the ISSM.
- Ensuring warning banners are placed on all monitors and appear when a user accesses a system.
- Ensuring system recovery processes are monitored and that security features and procedures are properly restored.
- Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.
- Formally notifying the ISSM and the DAA Rep/SCO when a system no longer processes classified information.
- Formally notifying the ISSM and the DAA Rep/SCO when changes occur that might affect accreditation/certification.
- Ensuring system security requirements are addressed during all phases of the system life cycle.
- Following procedures developed by the ISSM, in accordance with configuration management (CM) policies and practices, for authorizing software use prior to its implementation on a system. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM and appropriate approving authority prior to the change.
- Establishing audit trails and ensuring their review.
- Administering user identification (USERID) and authentication mechanisms of the IS or network.
- Ensuring the most feasible security safeguards and features are implemented for the IS or network.
- Ensuring no attempt is made to strain or test security mechanisms, or perform network line monitoring, or keystroke monitoring without appropriate authorization.
- Performing network monitoring for the purpose of identifying deficiencies, but only with approved software, and after notifying the ISSM and other appropriate authority.
- Accessing only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

1.5.10. (U) The Program Management Office (PMO)/Program Manager (PM).

- The PM/PMO shall be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

The responsibilities of the PMO/PM will include**:**

- Ensuring compliance with current IA policies, concepts, and measures when designing, procuring, adopting, and developing new ISs. This includes systems that are developed under contracts with vendors or computer services organizations and includes those systems that store, process, and/or transmit intelligence information.
- Ensuring that the Configuration Management process is addressed and used when new SCI ISs are under development, being procured, or delivered for operation. An integral part of configuration management is the System Accreditation process. Therefore, it is imperative that accreditation authorities be advised of configuration management decisions. This will ensure systems are fielded or modified within acceptable risk parameters and the latest security technology is being incorporated into system designs. This participation is most important at the Preliminary Design Review (PDR) and the Critical Design Review (CDR).
- Performing a risk assessment on the IS while under development and keep the risk assessment current throughout the acquisition development portion of the life cycle.
- Enforcing security controls that protect the IS during development.
- Ensuring all steps involved in the acquisition and delivery of a certifiable IS are followed. These include:
  - Evaluating interoperability with other systems.
  - Describing the IS mission so that it is clearly understood.
  - Determining the protection level of the new IS.

- Fully defining the security requirements for the IS. This must include any measures that have to be implemented to ensure the confidentiality, integrity, and availability of the information being processed.
- Formulating an approach for meeting the security requirements.
- Incorporating security requirements during system development.
- Developing accreditation Support documentation to be fielded with the IS.
- Ensuring the IS undergoes Certification and/or Accreditation (C&A) Testing and Evaluation (T&E) prior to operation.

1.5.11. (U) Privileged Users (e.g., System Administrator (SA)). The responsibilities inherent to IS administration are demanding, and require a thorough knowledge of the IS. These responsibilities include various administrative and communications processes that, when properly carried out, will result in effective IS utilization, adequate security parameters, and sound implementation of established IA policy and procedures. System administrators shall:

- Be U.S. citizens;
- Be IA trained and certified in compliance with DoD requirements; and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

In addition to the requirements for a general user, responsibilities of the system administration personnel shall include:

- Implementing the IS Security guidance and policies as provided by the ISSM/ISSO.
- Maintaining IS and networks to include all hardware and software (COTs/GOTs).
- Monitoring system performance ensuring that system recovery processes are monitored to ensure that security features and procedures are properly restored.
- Reporting all security-related incidents to the ISSM/ISSO.
- Ensuring that all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS.
- Performing equipment custodian duties by providing other system unique requirements that may be necessary. Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the accreditation/certification support documentation package.
- Maintaining software licenses and documentation.
- Notifying the ISSM/ISSO and the SCO formally when changes occur that might affect accreditation/certification.
- Ensuring Configuration Management (CM) for security-relevant IS software and hardware, to include IS warning banners, is maintained and documented.
- Monitoring hardware and software maintenance contracts.
- Establishing user identification (USERID) and authentication mechanisms of the IS or network and issue user logon identifications and passwords.
- Ensuring adequate network connectivity by ensuring that proper decisions are made concerning levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality for the system.
- Establishing audit trails and conducting reviews and archives as directed by the ISSM/ISSO.
- Providing backup of system operations.
- Assisting the ISSM/ISSO in developing and maintaining accreditation/certification support documentation package for system(s) for which they are responsible.
- Conducting periodic reviews to ensure compliance with the accreditation/certification support documentation package.
- Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.
- Formally notifying the ISSM/ISSO and the SCO when a system no longer processes classified information.
- Following procedures developed by the ISSM/ISSO, authorizing software use before implementation on the system.
- Assisting the ISSM/ISSO in maintaining configuration control of the systems and applications software ensuring the most feasible security safeguards and features are implemented on the IS or network.
- Prohibiting attempts to strain or test security mechanisms, or perform network line monitoring or keystroke monitoring without appropriate authorization.
- Performing network monitoring for the purpose of rectifying deficiencies, but only with approved software, and after notifying the ISSM and other appropriate authority and advising the ISSM/ISSO of security anomalies or integrity loopholes.
- Participating in the Information Systems Security incident reporting program and with the approval of the ISSM/ISSO, initiate protective or corrective measures when a security incident or vulnerability is discovered.

1.5.12. (U) General Users. General users must hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system. The responsibilities of a general user shall include:

- Using the system for official use, only. Appropriate personal use of IS must be approved first by the individual's supervisor.
- Participating, at a minimum, in annual computer security awareness briefings/training.
- Providing appropriate caveat and safeguard statements on all IS files, output products, and storage media.
- Protecting ISs and IS peripherals located in his/her respective areas.
- Safeguarding and reporting any unexpected or unrecognizable output products to the ISSO/SA as appropriate. This includes both display and printed products.
- Safeguarding and reporting the receipt of any media received through any channel to the appropriate ISSO/SA for subsequent virus inspection and inclusion into the media control procedures.
- Reporting all security incidents to the ISSO/SA or ISSM.
- Protecting passwords at the same level as the highest classification of material which the system is accredited to process.
- Protecting passwords by never writing passwords down and destroying the original password documentation following initial review.
- Protecting passwords from inadvertent disclosure.
- Protecting all files containing classified data.
- Notifying the system ISSO/SA if he or she suspects that a possible IS and/or network security problem exists.
- Ensuring access doors, covers, plates and TEMPEST seals are properly installed on ISs to eliminate security hazards.
- Protecting their authenticators and reporting any compromise or suspected compromise of an authenticator to the appropriate ISSO.

1.5.13. (U) Prohibited Activities. In general, there are activities which all users shall not perform on any Government systems:

- Use networked ISs for personal gain, personal profit or illegal activities.
- Release, disclose, or alter information without the consent of the data owner or the disclosure officer's approval. Violations may result in prosecution of military members under the Uniform Code of Military Justice, Article 92 or appropriate disciplinary action for civilian employees.
- Attempt to strain or test security mechanisms, or perform network line monitoring or keystroke monitoring without proper authorization.
- Attempt to bypass or circumvent computer security features or mechanisms. For example, when users leave their workstation unattended without using appropriate screenlock, other users shall not use the system.
- Modify the system equipment or software or use it in any manner other than its intended purpose.
- Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.
- Introduce malicious code into any IS or network and will comply with rules and regulations for scanning all magnetic media that he/she introduces, mails, or transports into or out of the organization.

1.6. (U) CONFIGURATION CONTROL BOARD (CCB) OVERSIGHT. This document is under the purview of a Joint Service CCB consisting of the Services SCOs, SCEs, and a representative from DIA, NSA and NIMA. Any recommended changes to the document should be forwarded to the appropriate CCB member.

1.7. (U) OTHER DOCUMENTATION SUPERSESSION. This document supersedes Supplement 1 to NSA/CSS Manual 130-1, Information System and Network Security Procedures for Service Cryptologic Elements (SCEs), current edition, and Joint DoDIIS/Cryptologic SCI Information Systems Security Standards, all previous editions.

CHAPTER 2
LIFE CYCLE SECURITY

2.1. (U) PURPOSE. The Director of Central Intelligence Directive (DCID) 6/3, for the Intelligence Community is used to provide a system of evaluating the degree of trust needed for an Information System (IS) processing classified and sensitive information. It is the basis for specifying security requirements in acquisition specifications, both for existing and planned systems. The Program Manager (PM), during acquisition, will require that security be an integral part of any contract used for acquisition consistent with the security requirements of the system. The PM and IS developers involved in the acquisition process of new ISs must ensure these new systems operate as intended and are accredited. They must ensure that systems are designed to meet user requirements, are developed economically, and contain appropriate security controls and audit trails. Procedures must be implemented and precisely followed to ensure new ISs are created and can be readily approved for operation at an acceptable level of risk. Acquisition procedures must address all aspects of IS development, to include the security requirements that must be met, the IS security features required, the IS operating environment, and a plan that properly tracks the process by which IS definition, development, and security testing are to take place. The purpose of this chapter is to address acquisition security requirements and includes:

- National security policy requirements as they pertain to system development.
- The responsibilities involved in the accreditation process.
- Levels of Concern and Protection Levels.
- Guidance that appropriate security requirements are identified early in the acquisition process.

2.2. (U) SCOPE. The early and complete identification of security requirements for an IS is a major security objective in all phases of the IS life cycle. These guidelines apply to all security personnel who must consider, improve, or change security throughout the life cycle to ensure continued adequate protection. These procedures are effective in the following life cycle phases:

	CONCEPTS DEVELOPMENT PHASE	YES
	DESIGN PHASE	YES
	DEVELOPMENT PHASE	YES
	DEPLOYMENT PHASE	YES
	OPERATIONS PHASE	YES
	RECERTIFICATION PHASE	YES
	DISPOSAL PHASE	YES

2.3. (U) PROCEDURES. Within each organization, life-cycle security requirements will be related to one of the seven life cycle phases which apply to all systems; Government owned, leased, or on loan from other organizations. Designated Approving Authority (DAA) Representatives (Reps)/Service Certifying Organizations (SCOs) must review and approve detailed system or subsystem security specifications.

2.3.1. (U) Concepts Development Phase. During the conceptual phase, security personnel must determine the data sensitivity and criticality of the IS being planned. This is accomplished by conducting sensitivity, risk/threat, interoperability, and economic assessments. The results of these assessments provide the data necessary to perform the analysis and design of the next phase. These guidelines apply to all personnel performing acquisition of ISs with the objective of fielding ISs with the appropriate security requirements identified early in the acquisition process.

2.3.1.1. (U) IS Security Design. The PMO/PM should ensure all IS security requirements are incorporated in the Critical Design Review, the System Security Plan (SSP)/Systems Security Authorization Agreement (SSAA) and the Security Concept of Operations (SECONOPS) (see DCID 6/3, 4.B.1.c.(1)). In concert with the Systems Design Security Officer (SDSO)/ Information Systems Security Engineer (ISSE), the PMO/PM will ensure the IS security design meets the requirements of DCID 6/3.

2.3.1.2. (U) Statement of Work (SOW) Requirements. The SOW will include a DD Form 254 and address contractor related issues pertaining to contractor personnel security, physical security, contractor ISs in support of the contract, TEMPEST requirements, and applicable security regulations. A Government official, either the SDSO/ISSE or DAA Rep/SCO, will coordinate these specific requirements depending on the particular acquisition.

2.3.1.3. (U) Additional Documentation. Additional documentation based on the system's identified Protection Level to include guide(s) or manual(s) for the system's privileged users (test plans, procedures and results) and a general user's guide may be required.

2.3.2. (U) Design Phase. During this phase of the life-cycle, the certification and accreditation process should begin. The DAA first determines the Levels of Concern (LOC) for Confidentiality, Availability, and Integrity based on the information characteristics determined in the Concepts Development Phase. The DAA then determines the required Protection Level for confidentiality based on the need-to-know, formal access approval(s), and clearance level(s), if applicable, of system users as compared to the sensitivity, formal compartments, and classification of the data to be stored, processed, or transmitted on the system. The Levels of Concern and Protection Levels are:

Security Features	Level of Concern	Protection Levels
Confidentiality	(Basic/Medium not used in Intelligence ISs) High	PL-1, PL-2, PL-3, PL-4, PL-5
Integrity	Basic, Medium, High	
Availability	Basic, Medium, High	

2.3.2.1. (U) Levels-of-Concern. Based on the characteristics of the information in the IS, a Level-of-Concern must be determined in each of three categories: confidentiality, integrity, and availability. The available Level-of-Concern ratings are Basic, Medium or High. The DAA determines the Level-of-Concern separately for each category based on the following:

- The Confidentiality Level-of-Concern rating for all ISs that process intelligence information is, by definition, High.
- The Integrity Level-of-Concern is determined by the necessary degree of resistance to unauthorized modification of the data in the IS. The greater the need for data integrity, the higher the Level of Concern.
- The Availability Level-of-Concern rating is based on the need of ready access to the system data. The greater the need for rapid data availability, the higher the Level-of-Concern.
- A detailed description of the determination and assignment of Levels-of-Concern can be found in DCID 6/3, section 3.B. and Table 3.1, with even greater detail of each category in Chapters 4 (Confidentiality), 5 (Integrity), and 6 (Availability).

2.3.2.2. (U) Protection Levels. The Protection Level of an IS is the implicit level of trust placed in the system's technical capabilities, and applies only to confidentiality. After determining that the Level-of-Concern for confidentiality must be high (since the system processes intelligence data), the DAA must then determine the necessary Protection Level based on:

- Required clearances,
- Formal access approval, and
- Need-to-know of all IS users.

2.3.2.2.1. (U) The DAA must explicitly determine the Protection Level for each IS to be accredited. DCID 6/3, Section 3.C. and Table 4.1 differentiate between the five Protection Levels (PL1 - PL5). Chapter 4 details the security features required for each Protection Level.

2.3.2.2.2. (U) The LOCs for Availability and Integrity and the PL for Confidentiality are identified using DCID 6/3 Chapters 4-6. During the design phase, the Project Management Office (PMO) develops the System Security Plan (SSP)/System Security Authorization Agreement (SSAA). This is a living document and should be updated throughout the IS's life cycle. It incorporates security documentation requirements found in DCID 6/3 and includes the mission need, system and environment description, intended system users, system security requirements, and development schedule. A template for the SSAA can be found in the DoD Intelligence Information System (DoDIIS) Security Certification and Accreditation Guide, Appendix D. A template for the SSP can be found in the NSA/CSS Information System Certification and Accreditation Process (NISCAP). The initial draft of the SSP/SSAA must be approved by the DAA Rep/SCO prior to system development. Actions must be taken by the Program Managers (PM) and SDSO/ISSE to ensure compliance with directives according to DCID 6/3.

2.3.3. (U) Development Phase. Adequate implementation of the necessary security measures is ensured during the development phase. The Development Security Manager, appointed by the PMO, has the major responsibility during the development phase. He should ensure a test plan is prepared and participate in all project meetings including site surveys. Security support from the certifying organization and/or DIA is required based on the Protection Level of the IS. Hardware, software, telecommunications and the entire operational environment must comply with the System Security Authorization Agreement (SSAA). This extends beyond the system itself; the proposed or existing facility that will house the system must be considered to ensure that proper physical security is available. During the development phase, design reviews may identify security considerations which were overlooked in the initial system design. If so, the SSAA must be updated accordingly. If major security considerations are discovered, the development may return to a previous phase for rework.

2.3.4. (U) Test, Certification and Accreditation Phase. During the test phase, the entire system is critically reviewed to ensure compliance with all specified security measures. A Security Test and Evaluation (ST&E) is conducted to certify that the system's security and contingency operations are properly implemented. Any shortcomings and/or vulnerabilities are identified, and a risk analysis is conducted. Based upon the outcome of the risk analysis, a plan addressing the shortcomings (fixes, work-arounds, etc.) is developed. All this is detailed in the Security Certification Test Report, which is used by the DAA when making the approval decision. A template for the Security Certification Test Report is located in the DoDIIS Security Configuration and Accreditation Guide, Appendix G. Following the resolution of any shortcomings, the conclusion of security testing, and after the appropriate Designated Approval Authority (DAA) grants accreditation approval, the system is released for operational use.

2.3.4.1. (U) Time Line for Certification Activities. A 90-day period is the basis for providing enough time for certifiers to properly prepare for and conduct a system certification evaluation and recommendation to the DAA. The 90 day timetable begins with the submission of the Request for Certification from the Program Manager (PM/PMO) to the Service Cryptologic Element (SCE)/Service Certification Office (SCO).

	90 days	60 days	30 days	0 days
PM Request for Certification/Accreditation	**X**			
SSP/SSAA	**X**			
SCE/SCO approval of SSP/SSAA		**X**		
SRTM & Test Procedures (SFUG if necessary)		**X**		
SCE/SCO approval of Test Procedures			**X**	
SCE/SCO submits Test Report and Test Memo				**X**

2.3.5. (U) Deployment and Operations Phase. Once the system is operational, the site operations staff and ISSO/ISSM are responsible for monitoring its security. They do this by controlling changes to the system via strict Configuration Management. IS users are responsible for operating the system in compliance with the security guidelines found in the SSP/SSAA. As required by DCID 6/3, the DAA Rep/SCO periodically reviews the adequacy of system security as required by all applicable regulations for unclassified, sensitive-unclassified, collateral, and SCI material. This review will take into account any system modifications and changes, including both hardware and software, to ensure that security requirements are adequate to meet any identified risks, threats to, or vulnerabilities of the system. All changes are updated in the SSP/SSAA as they occur. If any changes significantly affect the system's security posture, the DAA is notified so that the need for recertification can be determined.

2.3.6. (U) Recertification Phase. As required by the DAA, a system must be recertified whenever security changes occur in the LOC and PL, technical or non-technical security safeguards, threats to the system, operational environment, operational concept, interconnections, or any other significant increases in the level of residual risk. The recertification process includes: a review of existing security documentation to verify that these documents still accurately represent the system, a reevaluation of the system vulnerabilities, threat and risk, and a complete ST&E, or a subset of the original ST&E will be conducted. Even if no security-significant changes occur, recertification and accreditation of a system must be re-evaluated every three years after the issuance of an accreditation. Site Based accreditation provides for continued reevaluation.

2.3.7. (U) Disposal Phase. When an IS is no longer needed, disposition can occur in several ways: purging information residue from an IS or a component; releasing the IS or a component for reuse within the Intelligence Community; destroying an IS or a component through authorized channels; or, the method of shipment for an IS or component. All of the above actions must be approved by the DAA Rep/SCO. While emergency destruction of an IS is a possibility that occurs during the normal operational phase, it is considered a special case during the disposal phase.

CHAPTER 3

SIGNALS INTELLIGENCE (SIGINT) SYSTEMS ACCREDITATION PROCESS AND PROCEDURES

3.1. (U) PURPOSE. This chapter provides the accreditation processing requirements and procedures that, when implemented, will ensure Information Systems (ISs) do not operate without proper authority and effective security controls. All SIGINT ISs must be formally accredited or granted an approval-to-operate before they legally may be used to process, store, transmit, or receive data of any classification, to include sensitive-but-unclassified (SBU). This is in accordance with the NSA/CSS Information Systems Certification and Accreditation Process (NISCAP). Note: This chapter does not apply to intelligence information systems under the cognizance of the Director, Defense Intelligence Agency (DIA).

3.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

3.3. (U) DISCUSSION:

3.3.1. (U) Accreditation. Accreditation is the official authorization granted by the appropriate Designated Approving Authority (DAA), on a case-by-case basis, permitting the processing of information on an IS. Approval is based upon the DAA's review of the System Security Plan (SSP). Under certain conditions interim approval-to-operate (IATO) may be granted by the DAA/designee in accordance with section 9.D.4 of DCID 6/3.

3.3.2. (U) Configuration Management. The accreditation process and associated security concerns are integral to configuration management enforcement. Therefore, accreditation authorities will be included in configuration management decisions to ensure systems are fielded or modified within acceptable risk parameters and the latest security technology is incorporated into system designs. This participation is most important at the Preliminary Design Review (PDR) and the Critical Design Review (CDR). Where there is no formal configuration management process in an acquisition or system modification, the Program Manager (PM) will coordinate all relevant activities with the accreditation authority.

3.4. (U) ACCREDITATION IN GENERAL. Figure 3.1, General Accreditation Review and Approval Cycle, outlines the current cryptologic accreditation process. As the figure indicates, accreditation may be initiated from one of three different logical points: Unit, Service Cryptologic Element (SCE), and the National Security Agency (NSA)/Central Security Service (CSS).

3.4.1. (U) Formal Accreditation. Formal accreditation for any cryptologic IS can only be granted by the DAA, or DAA designee, after a site visit and only after a full test of the security controls of the entire system. This applies to ISs processing any classification level of information and those which may currently have an IATO.

3.4.2. (U) Issuing Accreditation. Once an SSP has been submitted and reviewed, the next step in the process is to issue accreditation/approval. The Information Systems Security Program Manager (ISSPM) and certain accrediting action officers have the authority to accredit all unclassified systems, collateral systems, and certain Sensitive Compartmented Information (SCI) systems within SCI Facilities (SCIFs). For certain systems, the ISSPM has the authority to issue accreditation on behalf of the NSA/CSS DAA.

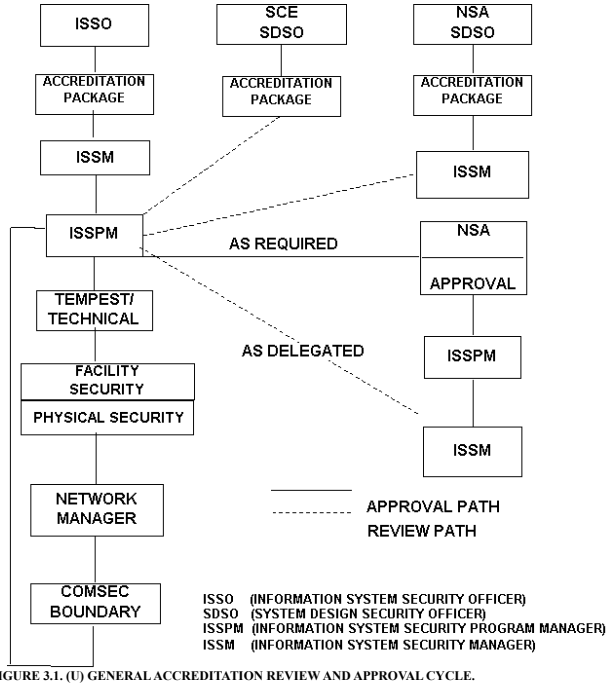


FIGURE 3.1. (U) GENERAL ACCREDITATION REVIEW AND APPROVAL CYCLE.

3.4.3. (U) Reaccreditation. When certain operational changes are made to an accredited IS, it must be submitted for reaccredidation by the Information System Security Officer (ISSO)/System Administrator (SA). If this is not done, the DAA may rescind the current accreditation. Reaccredidation is required when:

- The type of Central Processing Unit (CPU) and/or IS operating system changes.
- The IS is relocated to another area or TEMPEST zone.
- The IS Protection Level (PL) changes.
- The classification of material processed by the IS is changed.
- The IS is being connected to another IS or a network not previously connected.
- When users with a lower security clearance are added to the system.
- Any change to the IS which impacts security.

3.4.4. (U) Rescinding Accreditation. The DAA may cancel the accreditation of an operational IS if violations are found in the operational status of the IS. However, there are acceptable reasons for operational changes that do not normally constitute rescinding accreditation. Accreditation is not rescinded for:

- The substitution of similar components while components are in maintenance. However, if the original CPU is not returned to the IS when repair is completed, then an update to the SSP must be accomplished to reflect the correct serial numbers of the replacement CPU.
- The addition of new terminals, peripheral devices, or relocation of an IS providing the SSP is updated within 90 days to reflect the system additions or relocation. These actions can only be done with appropriate coordination (TEMPEST, Physical Security Office, etc.) and with Information Systems Security Manager (ISSM) approval.

3.4.5. (U) Accreditation 3-Year Anniversary Review. Each IS accreditation will be reviewed every 3 years. The ISSM is responsible for ensuring that recertification of each accredited IS is completed upon its 3-year anniversary. The SSP will be updated to reflect any undocumented changes and will be coordinated and forwarded to the appropriate DAA for approval.

3.4.6. (U) Authorized Exemptions From Accreditation. As stated, all ISs must be accredited before they may legally process any information. However, certain computers are never exposed to, contain, or process national security information (NSI) and are exempted from accreditation. The current approved list for accreditation exemptions is as follows:

- Computerized test equipment.
- Computers used in driving drill presses and their operations.
- Computers used in engraving devices or machines.

3.4.7. (U) IS Approval-to-Operate. Once an SSP has been submitted, you may receive an IATO or formal accreditation (see paragraph 3.1), based on the circumstances involved. The IATO is typically the first step in the accreditation process. An IATO may be granted based upon a preliminary review of the SSP. Upon review, temporary waivers may be granted, on a case-by-case basis, for the operation of an IS which has security deficiencies if the waiver supports the time-critical, mission-essential processing requirements. An IATO may be issued with an expiration date for temporary projects. Upon approval of the IATO, approval letters or messages are sent by the DAA directly to the organizational-level ISSM with information copies as necessary to ensure proper notification. The issuing of any approval is based upon the DAA's willingness to accept the risk for the IS based upon the documented evidence that adequate security measures have been taken to safeguard NSI. An IATO should not exceed 180 days. If required, an additional 180-day extension may be granted by the DAA Rep, but may not exceed 360 days.

3.4.8. (U) TEMPEST. Refer to Chapter 5 for applicable TEMPEST procedures involved with IS accreditation.

3.5. (U) ACCREDITATION PROCEDURES. It is imperative that all cryptologic ISs operate with appropriate approval and with the security controls necessary to protect the information they process. To ensure this is accomplished, well-defined and effective procedures must be established and followed.

3.5.1. (U) Accreditation Requests:

3.5.1.1. (U) Accreditation Requests Initiated at the Unit Level:

3.5.1.1.1. (U) The ISSO/SA obtains a new IS through channels such as supply, local purchase, or from the unit's Headquarters (HQ) through a planned program. The ISSO/SA completes an SSP for the new system and forwards it to the organization ISSM. The ISSM ensures proper organizational-level coordination with the SCIF manager for approval to use within the SCIF and with the TEMPEST officer for proper red/black installation. The ISSM coordinates with other local personnel as necessary to ensure that the SSP is properly coordinated. Once coordination is complete, and the package is approved at the unit level, the ISSM forwards the package to the DAA Rep for formal review.

3.5.1.1.2. (U) The DAA Rep reviews each SSP to ensure that adequate IS and network security measures have been implemented. The DAA Rep then coordinates with other personnel, as required, in the final approval process. Examples include, but are not limited to:

- A review by the TEMPEST Officer of each accreditation package to assess TEMPEST and technical security concerns.
- A review by the SCIF Manager or Physical Security Office to identify any facility security concerns.
- A review of the accreditation support documentation by the ISSM for proof of adequate network security measures and properly authorized connections.

3.5.1.1.3. (U) Following coordination, the SSP is then returned to the DAA Rep for final review and appropriate action. This is the critical point in the review process. If any non-concurrence exists, the SSP may be returned to the originator for correction. A non-concurrence can create an undesired delay in meeting a proposed operational capability. Therefore, it is important that the ISSM ensures the completeness and accuracy of each SSP before it leaves the organization.

3.5.1.2. (U) Accreditation Initiated Through Downward-Directed Programs. The other logical points from which an SSP may be generated and submitted relate to downward-directed programs. Within the SCEs, the DAA has the responsibility to ensure that all IS acquisitions are reviewed for IS and Network security concerns. A Systems Design Security Officer (SDSO) should be appointed to ensure that adequate built-in security capabilities are developed, tested, and implemented. This ensures that the new system is accreditable prior to its deployment. Ideally, the formal accreditation or an approval-to-operate should be delivered with the system at the time of installation. However, on occasion, ISs are fielded to NSA field sites by outside installation teams and often delivered without an SSP. This directly impacts the Initial Operational Capability (IOC) of the IS being delivered. To prevent this type of situation, unit involvement in the downward-directed program is critical to successful installation and operation of the IS.

It is unrealistic for an organization Commander/Commanding Officer and the ISSM/ISSO/SA to generate an SSP for these systems before the installation team departs the organization. However, without accreditation the newly fielded system cannot legally operate. To assist in eliminating this problem, the organization Commander/Commanding Officer will ensure the following guidelines are followed:

- The organization fielding the new system will be notified 90 days prior to the planned installation if an SSP has not been received. Ensure that survey teams understand the requirements of this chapter and that they must submit an SSP to the ISSM prior to their arrival for installation. The SSP will identify all communications connections to be made at the unit and must be coordinated with the DAA.
  NOTE: In implementing the provisions of NSA Directive 130-1 and its references, the organization Commander/Commanding Officer is authorized to deny access, or refuse country clearance, if overseas, to any team installing an IS being fielded without proper accreditation documentation.
- Coordination with the DAA and PM should be accomplished to determine the IS security impact of planned delivery of new ISs and/or changes to existing systems.
- Ensure that an ISSO/SA for the new system is assigned. The ISSM or ISSO/SA should be an active participant during all site survey team visits, upgrade meetings, etc.

3.5.1.3. (U) Accreditation at a Single-Service Site Including the Regional SIGINT Operation Centers. Processing of SSPs for ISs located at an organization controlled by only one military authority for SCIF management, TEMPEST, and IS and Network security will be handled by organization personnel through their chain of command. Accreditation of ISs belonging to a particular SCE can only be approved through the DAA/DAA Rep. At the RSOCs, a courtesy copy of the accreditation document will be provided to the parent service DAA.

3.5.1.4. (U) Accreditation at a Multi-Service Site. The processing of SSPs for ISs located at a SCE-site with two or more collocated SCE elements and controlled by one military authority (either an Air Intelligence Agency (AIA), Intelligence and Security Command (INSCOM), or Commander, Naval Security Group (COMNAVSECGRU) Commander/Commanding Officer), will follow the guidelines depicted in Figure 3.2.

The following rules apply:

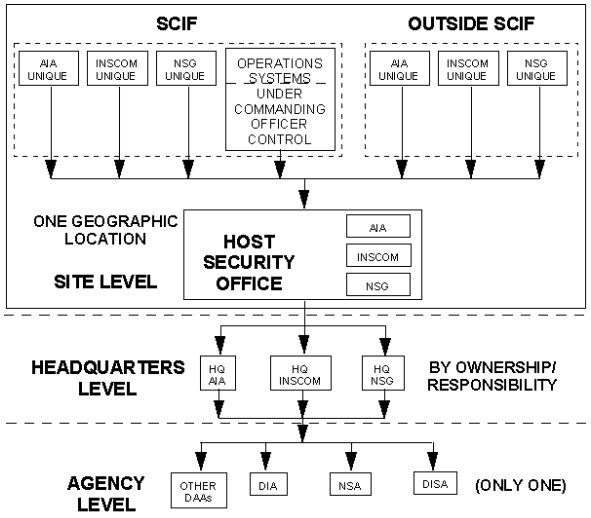


FIGURE 3.2 (U) MULTI-SERVICE ACCREDITATION

3.5.1.4.1. **(U) Operational Systems Under Control of the Commander/Commanding Officer**. All ISs directly supporting operations of the SCE-site, regardless of the functional user, are either under the ownership of, or the direct responsibility of the Commander/CO, regardless of his/her military affiliation. As such, all ISs supporting the direct mission of the site will be accredited by the DAA of the Commander/CO or the NSA/CSS SISSPM, as appropriate. This includes all ISs used for typical administrative support.

3.5.1.4.2. **(U) SCE Unique Systems Not Directly Supporting The Primary Mission**. The SSP on unique Mission ISs, belonging to a particular SCE, will be forwarded by the Host Security Office (HSO) to the SCE owning the IS. The owning SCE DAA will ensure the accreditation of the IS.

3.5.1.4.3. **(U) Assignment of a HSO at a Multi-Service Site**. Each multi-Service SCE site will assign a single office to perform the entire IS and Network security function for the site. All SSPs, regardless of the originating ISSO/SA, will be forwarded to the HSO for local review and coordination (See Figure 3.2). Once coordinated, the HSO will forward the SSP to the appropriate DAA to ensure proper approval. The HSO will maintain the complete database of all SSPs generated by the site.

3.5.1.5. (U) Accreditation by SCE Tenants Located at Non-SCE Interservice or Intercommand Sites. Accreditation of a cryptologic IS, functionally managed by any SCE, can only be approved by the appropriate DAA/DAA Rep, unless a separate written Memorandum of Understanding (MOU) provides different policy. The processing of SSPs for SCE ISs installed at interservice or intercommand sites will be handled according to the following procedures:

3.5.1.5.1. (U) The host Service is responsible for accreditation of the facility as a SCIF and facility TEMPEST certification. Therefore, the host Service facility manager and TEMPEST officer will be the coordinating authority on SSPs for cryptologic ISs located in facilities under their authority.

3.5.1.5.2. (U) The tenant organization functionally managing the cryptologic IS is responsible for obtaining accreditation through his/her chain of command. The HQ-level ISSPM will provide a copy of the IATO or final accreditation to the host Service facility manager and TEMPEST officer for their files.

3.5.2. (U) Submitting the SSP. Before full operation of the IS, and during the test phase, an SSP describing the IS must be prepared and submitted to the DAA/DAA Rep to document the IS use and the control mechanisms which are implemented to safeguard the system. The SSP should be submitted not later than 60-90 days prior to the desired IOC or as soon as the required information is known on specific components, configuration, and interfaces. On large ISs, where the purchase contract calls for a CDR, the SDSO should submit the package in the development phase immediately after the CDR. There are two ways of submitting SSPs; each is based upon organization requirements.

3.5.2.1. (U) Single Accreditation. This method of requesting accreditation is to submit only one IS accreditation per package. The reasons for submission vary, but range from the complexity of accrediting a large IS to the simplicity of being able to manage accountability easier by having only one IS accreditation per package. Under the Single Accreditation method there are no restrictions. For example, a system may be a standalone personal computer or any mainframe IS with personal computers being used as terminals or multiple personal computers connected on a local area network.

3.5.2.2. (U) Type Accreditation. This method permits the submission of one package requesting accreditation of multiple standalone ISs at one time. There are certain restrictions on a type accreditation submission. These restrictions are that all the ISs:

- Must be standalone and used for the same mission.
- Must be installed in the same general location.
- Are operating at the same protection level.
- Are processing the same data classification levels.
- Have the same basic hardware configuration.
- Are assigned to the same ISSO/SA.

3.5.2.3. (U) Format and Content. The acceptable format to present an SSP to the DAA/DAA Rep is the System Security Plan (SSP) Version 1.3, dated 11 October 2000.

3.5.3. (U) SSP and Database Classification. The classification of the accreditation database and an SSP, while directly related, are not necessarily the same. The following rules apply:

3.5.3.1. (U) Database Classification. The overall classification for the accreditation database is logically determined by the highest classification contained within any SSP in the database. The database may become classified SCI if the packages are independently classified at that level.

3.5.3.2. (FOUO) SSP Classification. An individual SSP may become classified for any of the following reasons:

- CONFIDENTIAL--If it contains a valid SIGINT Address (SIGAD).
- CONFIDENTIAL NOFORN--If it contains a valid TEMPEST zone in the building database.
- CONFIDENTIAL--If it pinpoints a particular building and room as being an SCI accredited area.

CHAPTER 4

DODIIS SITE-BASED ACCREDITATION AND SYSTEM CERTIFICATION

4.1. (U) PURPOSE. The DoDIIS Information Assurance Program has two components: The DoDIIS Systems Security Certification and Accreditation Process and the DoDIIS Site-Based Accreditation Methodology. This applies to all systems that process, store, or communicate intelligence information under the purview of the Director, DIA. Note: This chapter does not apply to intelligence information systems under the cognizance of the Director, National Security Agency/Chief, Central Security Service (NSA/CSS). The DoDIIS Systems Security Certification and Accreditation (C&A) Process addresses information systems being developed or undergoing modification that are evaluated prior to being fielded to DoDIIS sites. The DoDIIS Security Certification and Accreditation Guide describes the process for determining the appropriate security requirements that the new or modified system must meet, provides information on the requisite security documentation needed to support system security certification, and outlines the process for testing and fielding systems within the DoDIIS community. All Information Systems within DoDIIS will be tested and evaluated prior to achieving approval to operate or being granted formal certification and fielding to a DoDIIS site. The DoDIIS Site-Based Accreditation Methodology examines and establishes a baseline of all eligible information systems within a defined area, and designates this as a "Site". An Information System Security Manager (ISSM) is appointed by the Command authority for the site, and that individual, in coordination with the cognizant Certification Organization, manages all security related issues impacting the site's accredited baseline. Details of the Site-Based Accreditation Process can be found in DIA Manual (DIAM) 50-4.

4.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

4.3. (U) SYSTEM CERTIFICATION AND ACCREDITATION PROCEDURES:

4.3.1. (U) System Certification and Accreditation Compliance: The DoDIIS Security Certification and Accreditation Guide requires that all ISs be certified and accredited to ensure the IS meets the documented security requirements and that the security of the IS, as accredited, is maintained throughout its life cycle. The certification process validates that appropriate Levels-of-Concern for Integrity and Availability and an

appropriate Protection Level have been selected for the IS from the descriptions in DCID 6/3 and the required safeguards have been implemented on the IS as described in the associated security documentation. The DoDIIS security certification and accreditation process has been harmonized with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

4.3.2. (U) The System Certification and Accreditation Process:

4.3.2.1. (U) Phase 1. Definition - Focuses on understanding the IS requirement, the environment in which the IS will operate, the users of the IS, the security requirements that apply to the IS, and the level of effort necessary to achieve accreditation. The objective of Phase 1 is to agree on the intended system mission, security requirements, C&A boundary, schedule, level of effort, and resources required for the certification effort. This information is captured in the SSP/SSAA which is developed by the Program Manager.

4.3.2.2. (U) Phase 2. Development and Verification - Focuses on the system development activity and ensures that the system complies with the security requirements and constraints previously agreed during definition phase. This includes Beta-I system testing.

4.3.2.3. (U) Phase 3. Validation and Testing - Confirms compliance of the IS with the security requirements stated in the SSP/SSAA. The objective of this phase is to produce the required evidence to support the DAA in making an informed decision whether or not to grant approval to operate the system with an acceptable level of residual security risk. This includes Beta-II system testing.

4.3.2.4. (U) Phase 4. Post Accreditation - This phase starts after the system has been certified and accredited for operation. The Post Accreditation phase includes several activities to ensure an acceptable level of residual security risk is preserved. These activities include security documentation, configuration management, compliance validation reviews, and monitoring any changes to the system environment and operations. Changes to the security configuration of the system will require security review by the DAA.

4.4. (U) SITE-BASED ACCREDITATION METHOLODOGY:

4.4.1. (U) Site-Based Accreditation Methodology Compliance: The DoDIIS Site-Based Accreditation Process uses management techniques to assess risk by establishing a security domain called a "DoDIIS Site". This concept incorporates Site Security Management as a function of the DoDIIS Site's Configuration Management (CM) process. A DoDIIS Site Security Baseline defining the systems infrastructure is required, and any changes to the baseline must be documented in a timely manner. Before a DoDIIS site can establish a Site Security Baseline and be accredited, all system(s) must go through the security C&A process. The Site Security Baseline begins with the evaluation and accreditation of all individual ISs at the site. All ISs are then consolidated into this single management entity and evaluated as part of the security environment in which they operate. Site-Based Accreditation examines the ability of the organization to maintain a secure site baseline and environment. The maturity of site security policies, procedures, configuration management, system integration management, and risk management determines the site's ability to successfully establish and control a secure baseline. The certification process has a number of steps which, once successfully completed, will result in a Site Accreditation by the Director, Defense Intelligence Agency (DIRDIA), the Principal Accreditation Authority (PAA) for all DoDIIS Sites. DIAM 50-4 describes the step-by-step process to perform the Site-Based Accreditation and identifies documentation required to be maintained at the Site. Under Site-Based accreditation, intelligence mission applications entering the site will have already been certified by the responsible DAA Rep/SCO. All other agency systems are considered “Guest” systems at the site and are approved to operate as long as the agency has provided the appropriate documentation (see Chapter 21).

4.4.2. (U) The Site-Based Accreditation Process. The Site-Based Accreditation process consists of the following:

4.4.2.1. (U) Initial Site Visit (Initial Site Certification Visit). During this visit each site will be officially notified by the SCO that it was selected to undergo a Site-Based accreditation. A Certification Team will initiate the accreditation process by visiting the site. The purpose of this visit is to gather important baseline information. This function may be incorporated or combined in the Site Accreditation and Site Security and Engineering Certification Testing and Evaluation.

4.4.2.2. (U) Site Evaluation Visit (Site Security and Engineering Certification Testing and Evaluation and Site Accreditation). This visit will normally be conducted within 60-90 days following the Initial Site Certification Visit; however if the site has its site documentation, baseline, and security posture in order, it may be performed during the initial visit. It will consist of system security certification testing and/or security documentation review on each system.

4.4.2.3. (U) Site Compliance Visit (Vulnerability Assessment and Compliance Verification). This visit includes a vulnerability assessment of the networks, ISs, and linked operational elements. Assessments may be performed remotely or onsite. In addition, this periodic visit by the DAA Rep/SCO ensures that the site properly maintains control of the site security baseline. Vulnerability Assessment and Compliance Verification are normally conducted simultaneously as required.

4.5. (U) CONTRACTOR ACCREDITATION. Contractor facilities will not be site-based. Contractors should submit accreditation documentation in accordance with the National Industrial Security Program (NISP) Operating Manual (NISPOM).

4.6. (U) ACCREDITATION REVIEW. The ISSM is responsible for ensuring that the certification/recertification of each accredited IS is kept current based on the DoDIIS Security Certification and Accreditation Guide. The accreditation security documentation package will be updated to reflect any undocumented changes and will be coordinated and forwarded to the appropriate SCO.

4.7. (U) MINIMUM SECURITY REQUIREMENTS. All DoDIIS systems and networks processing SCI shall be protected according to DCID 6/3 by the continuous employment of appropriate administrative, environmental, and technical security measures. These measures will provide individual accountability, access control, enforcement of least privilege, auditing, labeling, and data integrity.

CHAPTER 5

TEMPEST

5.1. (U) PURPOSE. Information Systems (ISs), peripherals, associated data communications, and networks which may be used to process national security or security-related information may need to meet certain procurement and installation specifications as required by national TEMPEST policies and procedures applicable to the sensitivity level of the data being processed. This applies to all systems installed or planned. The objective of this area of security control is to minimize the risk of Hostile Intelligence Services (HOIS) exploiting unintentional emanations from intelligence systems. TEMPEST is a short name referring to investigations and studies of compromising emanations.

5.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

5.3. (U) DEFINITIONS. Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with National Security Telecommunications Information Systems Security Committee (NSTISSC)-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

- **Compromising Emanations.** Unintentional intelligence-bearing signals which if intercepted and analyzed disclose the national security information being transmitted, received, handled, or otherwise processed by any information processing equipment.
- **Inspectable Space.** The three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.
- **Routine Changes.** Changes which have a minimal effect on the overall TEMPEST security of the Sensitive Compartmented Information (SCI) Facility (SCIF). Adding a different type of electronic information processing equipment (unless the equipment added is known to have an unusually large TEMPEST profile), movement of the equipment within the facility, and minor installation changes are examples of routine changes.
- **Security Environment Changes.** Changes which have a detrimental effect on the facility. Changes to the inspectable space, addition of a radio transmitter or a modem for external communications, removal or reduction of an existing TEMPEST countermeasure (Radio Frequency Interference [RFI] Shielding, Filters, Control/Inspectable space, etc.) would be changes to the security environment.

5.4. (U) TEMPEST COMPLIANCE. All facilities processing SCI will be reviewed by a CTTA for initial TEMPEST accreditation and/or Inspectable Space according to National Security Telecommunications Information Systems Security Policy (NSTISSP) 300, National Policy on Control of Compromising Emanations, and National Security Telecommunications and Information Systems Instruction (NSTISSI) 7000, TEMPEST Countermeasures for Facilities. The CTTA is authorized to make acceptable risk determinations for specific facilities when justified.

5.5. (U) ACCREDITATION:

5.5.1. (U) TEMPEST Countermeasures Review. A CTTA must conduct or validate all TEMPEST countermeasure reviews. However, the requirement for a CTTA to conduct or validate such reviews does not imply the need to implement TEMPEST countermeasures. The recommended countermeasures will be threat driven and based on risk management principles. The inspectable space, as determined by a CTTA, will be the primary countermeasure.

5.5.2. (U) General Documentation. The local SCI security official will complete documentation in accordance with local TEMPEST Manager requirements. The local TEMPEST Manager will submit documentation in accordance with (IAW) service directives. A record of the TEMPEST security accreditation or inspectable space determination (ISD) will be retained within the SCIF.

5.5.3. (U) TEMPEST/ISD Accreditation. When an inspectable site houses multiple IS facilities and has a relatively protected and uniform TEMPEST security environment, the CTTA may grant a TEMPEST site accreditation or ISD for electronic processing of SCI. Each SCIF within the inspectable site must be evaluated separately on its own merits and cannot be approved automatically by being inside an inspectable space. The accreditation/ISD could range from a building to a base/post if all space is inspectable. Compliance is reported within the SCIF Fixed Facility Checklist.

5.6. (U) INSTALLATION REQUIREMENTS:

5.6.1. (U) All computer equipment and peripherals must meet the requirements of National Security Telecommunications Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92 and be installed IAW NSTISSAM TEMPEST/2-95, RED/BLACK separation criteria or as determined by a CTTA. The local TEMPEST Manager will oversee all such installations and coordinate on all accreditation documents resulting from the installation.

5.6.2. (U) Use all equipment as intended. All TEMPEST access doors, covers, and plates must be closed and fastened. Unauthorized modifications, even for testing purposes, are strictly forbidden.

5.6.3. (U) Additional TEMPEST requirements may exist if the equipment is not TEMPEST approved. In such a case, your local TEMPEST Manager should be contacted for further guidance.

5.6.4. (U) The local TEMPEST Manager must inspect all equipment installations.

5.6.5. (U) Special prohibitions and installation requirements exist for all transmitters, modems, and other networking and communications devices or equipment. Because of the broad range of this category, coordinate all requests for these devices with your local TEMPEST Manager.

5.6.6. (U) Do not consider a RED IS for any network which has any direct connection to a BLACK IS or other communications medium such as administrative telephone lines except through an approved cryptographic device.

5.6.7. (U) Do not use acoustically coupled modems and transmitters or locate them in any secure area without specific written approval from your Designated Approving Authority (DAA).

5.6.8. (U) You may use nonacoustic wireline modems with stand-alone, dedicated BLACK ISs providing that all appropriate telephone security requirements are met, consult with your local TEMPEST Manager.

CHAPTER 6

MINIMUM SECURITY REQUIREMENTS FOR USERS

6.1. (U) PURPOSE. The purpose of this chapter is to identify the minimum security requirements for a user of Information Systems. This chapter is designed so that it may be used as a general user reference for IS security training and awareness.

6.2. (U) SCOPE. Identifies the minimum security requirements for a general user necessary to operate an IS. These requirements are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

6.3. (U) MINIMUM SECURITY REQUIREMENTS. Users of ISs connected to networks shall use the system for official and appropriate use, only. Appropriate personal use of an IS must be approved by the user's supervisor.

6.3.1. (U) Identification and Authentication Requirements. Individual accountability is required for all users of IS that process SCI information. An IS user is identified through a unique User Identification (USERID) and a corresponding authenticator. The uniqueness of the USERID facilitates auditing and access controls. Group accounts (shared access through a single USERID) are prohibited unless a DAA approves this as an exception. An authenticator may be something the user knows, something the user possesses, or some physical characteristic about the user. The most common authenticator is a password. Users will comply with the following requirements to access IS:

6.3.1.1. (U) Users are required to login to all systems with a USERID and password.

6.3.1.2. (U) Users are required to logout of all systems at the end of each workday or for an extended absence.

6.3.1.3. (U) Protect Information against unattended operation. Protect information against unattended operation by locking your screen with a password protected screen saver/screen lock if the terminal is left unattended for any period of time. All systems are required to have a 15 minute timeout which invokes your password protected screen saver/screen lock if your terminal is left unattended for at least 15 minutes.

6.3.2. (U) Password Requirements. The following policy will be used when issuing, controlling, and changing passwords:

6.3.2.1. (U) Passwords must be at least eight alphanumeric mixed characters long.

6.3.2.2. (U) Upon initial logon (first time ever logged on to a system) the password must be changed.

6.3.2.3. (U) Users shall not share their passwords with other users.

6.3.2.4. (U) Passwords should not be easily associated with an individual. Do not use words found in a dictionary. Do not use nicknames, spouse names, street names, vanity plate names, parts of the SSAN, telephone number, etc.

6.3.2.5. (U) All passwords must be protected at the same security classification as the accreditation level of the IS.

6.3.2.6. (U) A password must be changed if it has been compromised or has been in use for six months or less. A user account will be deactivated when that account is idle for an extended period (recommend 60 days) or when the user departs for temporary duty for an extended period, is permanently transferred, has a change in need to know status or loses security clearance.

6.3.2.7. (U) Never write down passwords; destroy the original password documentation following initial review. Never type passwords onto an IS when being observed by other people.

6.3.2.8. (U) The following guidelines should be used when selecting a password:

DO:

- Include both upper and lower case characters.
- Include digits and punctuation marks.
- Include something which can be remembered without writing it down.
- Include combined words and characters (e.g. robot4my, eye-con).
- Consider special-acronyms (e.g. **Notf#swvw** - **N**one **o**f **t**his **f**ancy **#** **s**tuff **w**orks **v**ery **w**ell; or **A4PEGCED** - **A**ll **4** **P**rogrammers **E**at **G**reen **C**heese **E**very **D**ay).

DO NOT:

- Use any form of your logon name (e.g. initials).
- Use first, middle, last or maiden names.
- Use the name of a spouse, child, girl/boy friend.
- Use anything publicly available about you (e.g. address, car license plate number, car make, SSAN, etc.).
- Use all the same type of characters (e.g. 123245678, AAAAAAAA, etc.).
- Use a single word from a dictionary.
- Use substitution of characters by switching ones (1) for "ells" (l) or zeros (0) for "ohs" (o).
- Use names or characters from fantasy and science fiction stories (Quagmire, etc.).

6.3.3. (U) IS Warning Banner. All systems are required to display a logon warning banner. When the user logs on to a system, the user agrees to accept the conditions of the warning.

6.3.3.1. (U) A logon warning banner is required on all networked and standalone DoD interest computer systems (Government and contractor). The warning banner must be displayed before a successful logon and should include an option that allows the user to halt the logon process and a keystroke to continue processing. The intent of the banner is to confirm to the user that all data contained on DoD interest computer systems is subject to review by law enforcement authorities, DoD security personnel, and/or System Administrator, IAW Chapter 9. The banner is designed to inform all users, prior to accessing a DoD system, that by logging in they expressly consent to authorized monitoring.

6.3.3.2. (U) ISs supporting DoD operations have very specific warning banner requirements, and must include, at a minimum, the information shown in Figure 9.1.

6.3.3.3. (U) Whenever system administration personnel suspect that a system is being inappropriately used, either by authorized or unauthorized personnel, or some improper activity is being conducted, the matter will be reported immediately to the Information Systems Security Manager (ISSM).

6.3.4. (U) Configuration Requirements. The following policy will be used for the Configuration Management of all systems.

6.3.4.1. (U) Modifying, relocating, or reconfiguring the hardware of any computer system must be approved by the Configuration Control Board (CCB) or the Configuration Management Board (CMB) for your site. Hardware will not be connected to any system/network without the express written consent of the ISSM and the CMB/CCB. Examples of unauthorized hardware are: LAPTOP computers, PDA's, external peripherals, etc.

6.3.4.2. (U) Modifying, installing, or downloading of any software on any computer system may affect system accreditation and must be evaluated and approved by the ISSM with the local CMB/CCB.

6.3.4.2.1. **(U) Authorized Software.** Software that may be authorized includes that which has been:

- Provided officially by another U.S. Government Agency that has equivalent standards.
- Provided under contract to organizations involved with the processing of SCI and related intelligence information.
- Developed within a Government-approved facility.
- Provided through appropriate procurement channels, i.e. Commercial Off-the-Shelf (COTS) software.
- Distributed through official channels.
- Acquired from a reputable vendor for official use or evaluation (i.e. maintenance diagnostic software).

6.3.4.2.2. **(U) Unauthorized Software.** Types of software that are not authorized include:

- Games (See paragraph 11.6.).
- Public domain software or "shareware" which have been obtained from unofficial channels.
- Software applications that have been developed outside Government approved facilities, such as those developed on personally owned computers at home or software acquired via non-U.S. Government "bulletin boards".
- Personally owned software (either purchased or gratuitously acquired).
- Software purchased using employee funds (from an activity such as a coffee fund).
- Software from unknown sources.
- Illegally copied software in violation of copyright rules.
- Music and video or multimedia compact disks, not procured through official Government channels.

6.3.5. (U) Malicious Code Detection. Users of IS play a very important role in the prevention of malicious codes. For details, see Chapter 10. To actively participate in the prevention of malicious codes on an IS, users must be made aware of, and comply with, basic security requirements. Warnings and advisories frequently provide guidance on preventing infection from malicious code or viruses -- obey these. If a malicious code is detected or a presence of malicious code is suspected on any SCI IS, immediately report it to the ISSM for further instruction in accordance with Chapter 8. Do nothing that might cause the further spread of the malicious code.

6.3.6. (U) Virus Scanning Requirements. The user is responsible for ensuring that the following procedures are followed to minimize the risk of viruses:

- Use automated scanning applications, e.g., virus scanning, which will monitor media upon introduction to a system and data being transferred into the IS. If the media cannot be scanned then it is considered high risk and cannot be used on any SCI system without approval from the Service Certifying Organization (SCO).
- Check and review the IS operating environment for the presence of malicious code on a frequent basis.
- Avoid hostile mobile code through use of only authorized/verified and registered mobile code.
- Will not knowingly or willfully introduce malicious code into systems.
- Will not import or use unauthorized data, media, software, firmware, or hardware on systems.
- Will conduct screening of all incoming data (e.g., E-Mail and attachments) if this process is not automated.
- Will not use personal-owned media (e.g., music, video, or multimedia compact disks) in Government-owned IS.
- Will immediately report all security incidents and potential threats and vulnerabilities involving malicious code on ISs to the ISSM.

Note: Controlled Interfaces with malicious code scanning capability does not relieve the management of the receiving IS from the responsibility of also checking for malicious code.

6.3.7. (U) Information Storage Media. Removable information storage media and devices used with an Information System (IS) shall have external labels clearly indicating the classification of the information and applicable associated markings (e.g., digraphs, trigraphs). Examples include magnetic tape reels, cartridges, cassettes; removable discs, disc cartridges, disc packs, diskettes, magnetic cards and electro-optical (e.g.,

CD) media. Labeling exemption for operational security (OPSEC) requirements may be granted within local policy with DAA/DAA Rep/SCO concurrence. All removable information storage media and devices will be marked with the appropriate Standard Form (SF) 700-series classification and descriptor labels. These are:

- SF 706, Top Secret Label (Collateral only)
- SF 707, Secret Label (Collateral only)
- SF 708, Confidential Label (Collateral only)
- SF 710, Unclassified Label
- SF 711, Data Descriptor (On all magnetic media)
- SF 712, Classified SCI Label (All classification levels)

6.3.7.1. (U) Label Placement. See the Federal Register 2003 and applicable military department regulations for exact placement procedures. Labels will be affixed to all media in a manner that does not adversely affect operation of the equipment in which the media is used. Labels may be trimmed to fit the media. Labels for Compact Disks (CDs) must NOT be placed on the CD itself, but on the CD container or envelope. Record the accounting number in the "Control" block of the SF 711 and write the same number on the CD with a Paint-pen, CD labelmaker or permanent marker. The number should not interfere with the operation of the CD. Notice: Do not use pens that contain toluene.

6.3.7.2. (U) Data Descriptor Label. The SF 711, Data Descriptor Label, is used to identify the content of a specific media to include unclassified, collateral-classified, and Sensitive Compartmented Information (SCI). An SF 711 is not required if the disk bears the following information: Organization, office symbol, classification, and media sequence number (if locally required). The user fills in the "Classification", "Dissem", "Control", and "Compartments/Codewords" blocks as appropriate.

6.3.7.3. (U) Classification Markings. All documents residing or processed on information storage media/ISs will be marked in accordance with Director of Central Intelligence (DCI) Directive (DCID) 6/3, Sensitive Compartmented Information Administrative Security Manual, or appropriate Service regulations.

6.3.7.4. (U) Control and Accounting of Media. For any system that operates with PL-3 or lower functionality, media which is not write-protected and is placed into that system must be classified at the highest level of information on the system until reviewed and validated. Media accountability will be based on the determined classification level of the media.

6.3.7.4.1. **(U) Information Storage Media Control.** In addition to the labeling of information storage media according to Chapter 13, there is a requirement to control and account for certain information storage media within functional categories. The organization Commander/CO/SIO is responsible for development of a unit-level Standard Operating Procedure (SOP) for control and accountability of media.

6.3.7.4.2. **(U) Inspections.** The organization must be able to demonstrate positive control and accounting of information storage media according to its SOP when reviewed by inspection authorities.

6.3.7.4.3. **(U) Control Procedures.** Control of information storage media should begin upon introduction into the organization according to the SOP.

6.3.7.4.3.1. (U) Information storage media accountability is required for Top Secret BRAVO and permanent Collateral Top Secret files.

6.3.7.4.3.2. (U) Information storage accountability as a security protection measure is eliminated for collateral classified information (to include Top Secret non-permanent files), all classification levels of Special Intelligence (SI) (to include GAMMA and ENDSEAL), Talent-Keyhole (TK), and BRAVO material below Top Secret.

6.3.7.4.3.3. (U) Requirements for controls of specific Special Access Program (SAP) information will be defined by the respective Program Manager.

6.3.7.4.4. **(U) Other Categories of Storage media.** The following major categories of information storage media should be considered for accountability control in compliance with copyright and licensing with procedures documented in the SOP:

- Commercial Off-The-Shelf (COTS) and vendor software.
- Government developed software.
- Other organization unique software and data.

6.3.8. (U) Hardware Labeling Requirements. Labels will be displayed on all components of an IS, including input/output devices that have the potential for retaining information, terminals, standalone microprocessors, and word processors used as terminals, bear conspicuous external labels stating the highest classification level and most restrictive classification category of the information accessible to the components in the IS. The labels should be the standard form (SF) 700 series media classification labels or equivalent. The labeling may consist of permanent markings on the component or a sign placed on the terminal.

6.3.9. (U) Security Training Requirements. An integral part of the IS security program is the mandatory training required by public law. Users shall receive initial training on prescribed IS security restrictions and safeguards prior to accessing corporate IS assets. General users require system security training to safeguard systems and information on those systems/networks. As a follow-up to this initial training, users must be provided, and actively participate in an ongoing security education, training, and awareness program which will keep them cognizant of system changes and associated security requirements as they occur. General users training will include but is not limited to the following:

- An awareness of system threats, vulnerabilities, risks, system data, and access controls associated with the IS being used.
- How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes).
- How to protect authenticators and operate the applicable system security features (e.g., setting access control rights to files created by user).
- How to recognize and report security violations and incidents, see Chapter 8.

6.3.9.1. (U) Security Awareness and Training Program. The key to protecting Information Systems (ISs) & Networks and the information they process is the development of an effective Security, Education, Training and Awareness Program. The program is intended to provide two levels of knowledge:

6.3.9.1.1. **(U) Awareness Level.** Creates a sensitivity to the threats and vulnerabilities of national security information systems, and a recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices in IA. Awareness level training will be conducted when:

- In-processing. Site specific information will be briefed based on the mission and the requirement of the job responsibility.
- Receipt of USERID and Password. Privilege User/ISSO will brief the user on his/her responsibilities.
- Annual Awareness Refresher Training. Classroom, Briefings, Computer Based Training, or Seminars will be used and documented to ensure all users comply with this requirement.

6.3.9.1.2. **(U) Performance Level.** Provides the employee with the skill or ability to design, execute, or evaluate agency IA security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks.

6.3.10. (U) Destruction of Media. When destruction of information storage media is required, it must be accomplished in accordance with approved procedures and the organization's media accounting system must be updated to reflect this change. See Chapter 20, Paragraph 20.4.5. Destroying Media, for additional guidance.

6.3.10.1. (U) Destruction certificates are required for accountable material and will be retained as a permanent record.

6.3.10.2. (U) Non-accountable material no longer requires destruction certificates.

6.3.11. (U) Information Transfer and Accounting Procedures. Users should be knowledgeable of procedures for the transfer of information or software among Information Systems (ISs) of different classification levels using information storage media. The procedures are intended to protect the confidentiality of information on the media as well as other data on the end-point IS at different levels, prevent transfers of malicious code (Chapter 10 is germane), and prevent violation of legal copyright or license rights. For any system that operates with PL-3 and below functionality, media which is placed into that system must be classified at the highest level of information on the system until reviewed and validated. See Chapter 18.

CHAPTER 7

SECURITY GUIDELINES FOR THE PRIVILEGED AND GENERAL USER

7.1. (U) PURPOSE. The Privileged User is assigned by management personnel (at NSA/CSS the Office of Security approves Privileged Users) and is the single point of contact for the administration of a specifically defined Information System (IS). The privileged user is responsible for maintaining the IS throughout day-to-day operations, ensuring that the system operates within established accreditation criteria, and keeping the system in an operational mode for general users. System administration personnel are the primary interface between the users of an IS and the organization's Information Systems Security (ISS) management personnel. This chapter provides the privileged user with the security guidance and procedures necessary to implement an effective System Administration program.

7.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

7.3. (U) SECURITY TRAINING. The individual assigned the responsibility for IS administration must be knowledgeable in the basic security concepts and procedures necessary to effectively monitor IS activity and the environment in which it operates. To satisfy these requirements, General users require different training than those employees with specialized responsibilities:

7.3.1. (U) General Users training. General users training will include but is not limited to the following:

7.3.1.1. (U) How to protect the physical area, media, and equipment (e.g., locking doors, care of diskettes).

7.3.1.2. (U) How to protect authenticators and operate the applicable system security features (e.g., setting access control rights to files created by user).

7.3.1.3. (U) How to recognize and report security violations and incidents.

7.3.1.4. (U) The organization's policy for protecting information and systems.

7.3.2. (U) Privileged Users training. Privileged users training will include but is not limited to the following:

7.3.2.1. (U) How to protect the physical area, media, and equipment (e.g. locking doors, care of diskettes, etc.)

7.3.2.2. (U) Understand security consequences and costs so that security can be factored into their decisions.

7.3.2.3. (U) Have a thorough understanding of the organization's policy for protecting information and systems, and the roles and responsibilities of various organizational units with which they may have to interact.

7.3.2.4. (U) Have a thorough understanding of system security regulations and policies.

7.3.2.5. (U) Be aware of what constitutes misuse or abuse of system privileges.

7.3.2.6. (U) Have an understanding of how to protect passwords, or other authentication devices, and be familiar with operating system security features of the system.

7.3.2.7. (U) Know how to recognize and report potential security vulnerabilities, threats, security violations, or incidents.

7.3.2.8. (U) Understand how to implement and use specific access control products.

7.3.2.9. (U) Have an understanding of how to protect the media and equipment (e.g. system maintenance and backup, care of diskettes).

7.3.2.10. (U) How to protect authenticators and operate the applicable system security features.

7.3.3. (U) Security Awareness and Training Program. The key to protecting Information Systems (ISs) & Networks and the information they process is the development of an effective Security, Education, Training and Awareness Program. The program is intended to provide two levels of knowledge:

7.3.3.1 (U) Awareness Level. Creates a sensitivity to the threats and vulnerabilities of national security information systems, and a recognition of the need to protect data, information and the means of processing them; and builds a working knowledge of principles and practices in IA. Awareness level training will be conducted when:

- Inprocessing. Site specific information will be briefed based on the mission and the requirement of the job responsibility.
- Receipt of USERID and Password. Privilege User/ISSO will brief the user on his/her responsibilities.
- Annual Awareness Refresher Training. Classroom, Briefings, Computer Based Training, or Seminars will be used and documented to ensure all users comply with this requirement.

7.3.3.2. (U) Performance Level. Provides the employee with the skill or ability to design, execute, or evaluate agency IA security procedures and practices. This level of understanding will ensure that employees are able to apply security concepts while performing their tasks.

7.4. (U) PROCEDURES. Sensitive Compartmented Information (SCI) IA doctrine requires many security relevant actions to properly implement a secure environment to protect national interest information. The following procedures outline several items that apply to all SCI ISs and must be given full consideration by system administration personnel.

7.4.1. (U) Identification and Authentication Requirements. User Identification (USERIDs) are used for identification of a specific user on the IS to facilitate auditing. Group accounts are generally prohibited; exceptions to this policy shall be approved by the Designated Approving Authority (DAA)/Service Certifying Organization (SCO). Passwords (as authenticators) are used to provide an access path for authorized users while denying access to the unauthorized user. Use the following procedures to generate, issue and control USERIDs and passwords:

7.4.1.1. (U) Documenting USERIDs and Passwords. USERIDs and passwords are issued to personnel requiring access to information via a particular IS, but only if the proposed user has the same clearance level of that information and the required need-to-know. To document the issuing of USERIDs and passwords use a National Security Agency/Central Security Service (NSA/CSS) Form G6521, Access Request and Verification, (National Stock Number [NSN] 7540-FM-001-3448), or similar form. See Figure 7.1.

SECURITY CLASSIFICATION

ACCESS REQUEST AND VERIFICATION

INSTRUCTIONS
Complete one form for each person, for each AIS to be accessed. The ISSO will retain this form for 30 days after access removal.
The Functional Manager will ensure prompt removal of all unauthorized personnel.

PART 1. TO BE COMPLETED BY INDIVIDUAL REQUESTER

1. TYPE OR PRINT NAME (Last, First, MI)	2. GRADE OR RANK	3. SSN
4. CLEARANCE/ACCESS AUTHORIZED	5. ORGANIZATION/OFFICE SYMBOL	
6. ORGANIZATION ADDRESS		7. PHONE (Comm /DSN)
8. SYSTEM TO BE ACCESSED	9. TYPE OF REQUEST (User Access) ☐ ADD ☐ MODIFY ☐ DELETE	
10. TYPE USER ☐ OPERATOR ☐ AUDITOR ☐ U.S. CITIZEN ☐ DB ADMIN ☐ APPL PROGRAMMER ☐ OTHER (SPECIFY) ☐ CONTRACTOR ☐ SYSTEM PROGRAMMER	11. ACCESS REQUIREMENTS	
12. ISSO ORGANIZATION AND ADDRESS		

PART 2. IDENTIFICATION OF FUNCTIONAL AREA MANAGER

I certify all of the above information is true and correct. Additionally, I existing or modifying personnel access, I certify that the above individual holds the required clearance, has a valid "need to know" to the specified data/server, and is authorized access to the data listed

13. PRINT OR TYPE FUNCTIONAL AREA MANAGER (Name and Title)	14. OFFICE SYMBOL	15. PHONE (Comm /DSN)
16. SIGNATURE		17. DATE OF REQUEST

PART 3. TO BE COMPLETED BY THE INFORMATION SYSTEMS SECURITY OFFICER

18. REQUEST ☐ APPROVED ☐ DISAPPROVED (If disapproved, specify reason)	
19. ASSIGNED USERID	20. DATE ACCESS AUTHORIZED (Deletion/Modified)
21. INFORMATION SYSTEMS SECURITY OFFICER (Name and Grade)	22. OFFICE SYMBOL
23. SIGNATURE	24. PHONE (Comm /DSN)

PART 4. TO BE COMPLETED BY REQUESTER UPON RECEIPT OF USERID/PASSWORD

I acknowledge receipt of my assigned USERID/PASSWORD for the above AIS and I am aware of my user responsibilities listed
1. I must protect my password as required by National Security
2. I must report changes in my status promptly, in writing, to the ISSO or my functional area manager (for example, TDY of 60 days more, POA or POS, removal of security access, or changes in the requirements for "need to know").
3. My access required must be semiannually reestablished.
4. Frequent changes of passwords are necessary. The ISSO must change the password every
5. I understand that the ISSO has the right to revoke my access and to inspect all files which I
6. I consent to any authorized monitoring IAW DoD direction.

25. SIGNATURE	26. DATE OF RECEIPT

FORM G6521 REV MAR 95 (Supersedes G6521 Nov 92 which is obsolete)
NSN: 7540-FM-001-3448

SECURITY CLASSIFICATION

FIGURE 7.1 (U) SAMPLE FORM

NOTE: Do Not include any assigned passwords on the roster. The SA may actually perform these duties for the ISSM, however, the ISSM still maintains responsibility.

7.4.1.2. (U) USERID and Password Issuing Authority and Accountability. The Information Systems Security Manager (ISSM), or designee, is the official authorized to issue the initial USERID and password to each user of the system. The ISSM/designee will maintain a current user account roster for each system for which they are responsible, to include the names of authorized maintenance personnel. The roster will contain, at a minimum, each user's:

- Full name, grade or rank, and Social Security Account Number (SSAN).
- Organization, office symbol, and telephone number.
- USERID.

7.4.1.3. (U) Supervisor Authorization. Obtaining supervisor approval for each individual requiring IS access. The privileged user must ensure that all individual access authorizations are valid, need-to-know is established and access is work-related.

7.4.1.4. (U) Access Requirements Validation. The privileged user will provide each functional area within the organization with a current general user roster (for that functional area only) and require that the supervisor validate all access requirements annually at a minimum. The annual validation process will be documented.

7.4.2. (U) Control Guidelines. Use the sample form in this chapter, or similar Access Request and Verification form, to request access, validate clearances and need-to-know, issue USERID and passwords, and control the removal of personnel from ISs when access is no longer authorized.

7.4.2.1. (U) The form may be classified based on the information contained therein. It is the responsibility of the individual's supervisor to ensure that all copies of the form are appropriately classified.

7.4.2.2. (U) Never enter the assigned password of an individual on the form used to establish a user's account. The issuing ISSM/SA will distribute the initial password in a secure manner. The requesting individual must authenticate on the form that a password has been received, and the signed form must be returned to the ISSM/SA before activation of the account. The form will be retained by the ISSM/SA for a minimum of one year after access is removed.

7.4.3. (U) System Access Removal Procedures. Access removals from an IS must be accomplished using a form similar to the Figure 7.1 Access Request and Verification form. If the Commander/Commanding Officer, or designee, determines an individual's access to a system or database should be terminated, the Commander/Commanding Officer, or designee, will sign the removal document.

7.4.4. (U) Audit Trail Requirements. An audit trail capability must exist to obtain formal accreditation of an IS. The audit trail should be automated, and provide permanent on-line or off-line storage of audit data separate from data files.

7.4.4.1. (U) Automated Audit Trail Information Requirements. ISs approved for classified processing should contain, at a minimum, the following audit trail records:

- **Login/logout (unsuccessful and successful).**
  - Auditing of successful login and logout events is key to individual accountability. Unsuccessful login attempts may be evidence of attempted penetration attacks. Logins and logouts shall be audited by the underlying operating system. In addition, the syslog mechanism may be used to notify an ISSM/SA of an unsuccessful login attempt.
  - Audit data should include date, time, USERID, system ID, workstation ID, and indication of success or failure.
- **Use of privileged commands (unsuccessful and successful).**
  - Privileged commands are commands not required for general use, such as those that manage security-relevant data and those that manage an application. In UNIX workstations, these commands include, for example, the SU command, which is used to become the root user. The UNIX root user has access to all information stored on the system. Such commands must be accessible only to persons whose responsibilities require their use.
  - The ISSM/SA shall select the privileged commands (i.e., commands normally executed by the root user) to be audited. This event can be audited via the underlying operating system or application audit.
  - Audit data should include date, time, USERID, command, security-relevant command parameters, and indication of success or failure.
- **Application and session initiation (unsuccessful and successful).**
  - The use of application programs and the initiation of communications sessions with local or remote hosts are audited to provide the ISSM/SA a general history of a user's actions. An unsuccessful attempt to use an application or initiate a host session may indicate a user attempting to exceed his or her access authorizations. This event should be audited via application audit.
  - Audit data should include date, time, USERID, workstation ID, application ID, and indication of success or failure.
- **Use of print command (unsuccessful and successful).**

- The printing of classified and sensitive unclassified information is audited to maintain accountability for these materials. Print commands and the identity of the printed material should be audited via application audit.
- Audit data should include date, time, USERID, and destination.

- **Discretionary Access Control (DAC) permission modification (unsuccessful and successful).**
  - The changing of DAC permissions on files or directories should be audited since it could result in violations of need-to-know. This event can be audited via the underlying operating system and/or application audit.
  - Audit data should include date, time, user (requester) ID, user/group ID (to whom change applies), object ID, permissions requested, and indication of success or failure.
- **Export to media (successful).**
  - The copying of files to removable media should be audited to maintain accountability of classified materials. Removable storage media have large capacity and could potentially disclose large amounts of information. This event can be audited via the underlying operating system and/or application audit.
  - Audit data should include date, time, USERID, source and destination file IDs, system ID, and device ID.
- **Unauthorized access attempts to files (unsuccessful).**
  - An attempt to access files in violation of DAC permissions could indicate user browsing and must be audited. This event can be audited via the underlying operating system and/or application audit.
  - Audit data should include date, time, USERID, system ID, and file ID.
- **System startup/shutdown.**
  - System startup and shutdown shall be monitored and be auditable. This event should be audited by the operating system.
  - Audit data should include date, time, USERID, system ID, and device ID.

7.4.4.2. (U) Manual Audit Trail Implementation. If Automated Audit Trails are not supported, the ISSM/SA must obtain approval from the ISSPM/SCO to conduct manual audits. At a minimum, manual audits will include:

- The date.
- Identification of the user.
- Time the user logs on and off the system.
- Function(s) performed.

7.4.4.3. (U) Products of Audit Trail Information. Audit trail products should be handled as follows:

7.4.4.3.1. (U) Classify and protect audit trail information according to the security classification level of information contained in the audit.

7.4.4.3.2. (U) If hardcopy audit trail products are generated on an IS, print them on continuous paper whenever possible. If continuous paper is not used, all pages will be numbered with a sequence number on each printed line. This is required to protect the integrity of the audit trail data**.**

7.4.4.3.3. (U) Where possible, to reduce workload, generate summary reports which reflect system abnormalities, who performed what function, and to what database, rather than listing the entire audit trail.

7.4.4.4. (U) Audit Trail Checks and Reviews. The ISSO/SA will review the audit trail logs (manual and automated), or summary reports, to verify that all pertinent activity is properly recorded and appropriate action has been taken to correct and report any identified problems. Paragraphs 7.4.4.1 and 7.4.4.2 list audit trail requirements. Audit trail logs or summary reports shall be reviewed weekly, at a minimum, or as directed by the ISSM.

7.4.4.5. (U) Audit Trail Records Retention. Retain Audit Trail records for five years and review at least weekly.

7.4.5. (U) Automatic Log Out Requirements. The privileged user should implement an automatic logout from the IS when the user leaves his/her terminal for an extended period of time. This should not be considered a substitute for logging out (unless a mechanism actually logs out the user when the user idle time is exceeded).

7.4.6. (U) Limited Access Attempts. An IS will be configured to limit the number of consecutive failed access attempts to no more than five; three is recommended.

7.4.7. (U) Use of Windows Screen Locks. Screen locks are mandatory, and require a password for reentry into the system. If an IS is idle for 15 minutes, the screen lock shall be activated. Screen locks are not authorized in lieu of log-off procedures. Operations may require exceptions which must be approved by the ISSPM/SCO.

7.4.8. (U) Testing, Straining, and Hacking. SCI IA policy states that testing, straining, hacking, or otherwise attempting to defeat or circumvent the security measures of an operational IS or network is prohibited without authorization. The privileged user must ensure that submitting a request through the ISSM to the DAA Rep/SCO approves such activities. All such approvals must be in writing and limited to an explicit assessment.

7.4.9. (U) Warning Banners. A logon warning banner is required on all networked and standalone Department of Defense (DoD) computer systems (Government and contractor). The warning banner must be displayed and acknowledged before a successful logon. Refer to Chapter 9 for complete instructions on the implementation of warning banners.

7.4.10. (U) Network Monitoring:

7.4.10.1. (U) Maintenance Monitoring. Privileged users/network technicians may use Local Area Network (LAN) analyzers or "sniffers" to monitor network traffic provided:

- Reasonable notice has been provided to all users by display of the warning banners (Paragraph 7.5.10).
- The base or post has been certified for monitoring by the Service General Counsel (if required by the appropriate Service).
- The sniffer or monitor does not intercept any traffic from outside the military base or post.
- The privileged user has received approval from the DAA Rep/SCO (or NSA/CSS SISSPM) to monitor in the normal course of his or her employment while engaged in activity necessary incident to the rendition of his or her service or to the protection of the rights or property of the communications network (the provider of the network service) except that this monitoring is only permitted for service or mechanical quality control checks.

7.4.10.1.1. (U) Network traffic monitoring may not last longer than is necessary to observe transmission quality.

7.4.10.1.2. (U) No permanent recording of the network monitoring activity may be made.

7.4.10.1.3. (U) Monitoring traffic on civilian networks is strictly prohibited and may result in criminal and civil liability under the Computer Fraud and Abuse Act, 18 U.S. Code section 1030 and the Electronic Communications Privacy Act, 18 U.S. Code Section 2510 and following.

7.4.10.2. (U) Targeted Monitoring. Unauthorized targeted monitoring of a particular individual, machine or group is prohibited. When service quality or transmission quality monitoring reveals suspicious activity, including hacking or misuse, monitoring must cease and appropriate officials informed. At a minimum, notify the Commander/Commanding Officer, or his/her designated representative, and the ISSM. Privileged users may, of course, always terminate any connection at any time when the safety or property of the network is endangered. privileged users shall cooperate with law enforcement and security officials in accordance with applicable Service guidelines. Notify the DAA Rep/SCO of any planned targeted monitoring (see 9.3.3.).

CHAPTER 8

INFORMATION SYSTEMS (IS) INCIDENT REPORTING

8.1. (U) PURPOSE. Incidents may result from accidental or deliberate actions on the part of a user or occur outside of the organization as well. An accidental incident should be handled administratively. Evidence of criminal activity from a deliberate action should be treated with care, and maintained under the purview of cognizant law enforcement personnel (see Chapter 9 "Information System Monitoring Activities" for specific guidance). All management personnel must ensure that IS users are aware of the policy governing unauthorized use of computer resources. When it is suspected that an IS has been penetrated, or at any time system security is not maintained, it must be reported both within the organization and to the appropriate external authorities for action. Any use for other than authorized purposes violates security policy, and may result in disciplinary action under the Uniform Code of Military Justice (UCMJ) and/or other administrative directives. This chapter provides procedures for formal incident reporting.

8.2. (U) SCOPE. These procedures are effective in the following life-cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

8.3. (U) PROCEDURES. Discovery of a viral infection, introduction of malicious code, hacker activity, system vulnerabilities, or any unusual happenings will be reported immediately to the ISSM and an investigation initiated. Accidental incidents (for example, a one time brief Web site visit containing inappropriate content or inappropriate or vulgar usage of mission systems chat features) or other minor infractions can be handled administratively within the unit. Make every effort to contact the data owner to obtain specific guidance to afford minimum acceptable protection in cases of spillage and compromise.

8.3.1. (U) Reporting Process. Using the ISSM/ISSO or SA as appropriate, the Commander/Commanding Officer must report all abnormal security events to the proper authority. Incident reporting should be accomplished by each service through their appropriate ISSM or security channel, such as the Service Certifying Organization (SCO). IA computer security reporting should be done in conjunction with (but not exclusive of) the physical security reporting chain. The ISSM should work closely with the physical security manager to resolve these incidents.

8.3.2. (U) Types of IS Incidents and Reports. The following are examples of incidents that must be reported:

- **Compromise or Probable Compromise.** Examples of these are: Missing accountable media; human error in reviewing media for content and classification, resulting in compromise; and incorrect setting of a security filter, resulting in compromise.
- **Spillage.** Information of a higher classification or restrictive in nature intentionally or inadvertently placed on machines or networks of lower or less restrictive policy.
- **External Hacker Activity.** Activity where a hacker is operating from an outside location by using some network and he/she is not physically resident at the location where the activity is being observed.
- **Internal Hacker Activity.** Activity where a hacker is operating from within the site where the activity is being observed. **Caution:** if the hacker is suspected of monitoring the Automatic Digital Network (AUTODIN)/Defense Message Messaging System (DMS) message traffic, do not use AUTODIN/DMS to send the report. Instead, send the report by facsimile to the required addressees, followed up by a phone call to confirm receipt of the report.
- **Malicious Code.** Any potentially hazardous or destructive computer code other than a virus, such as a logic bomb, worm or TROJAN horse. **NOTE:** malicious code will probably also represent a vulnerability, as described below.
- **Unauthorized Monitoring.** Any individual or group of individuals found to be monitoring an IS without written authority from security officials.
- **Virus Actual infection.** A known active attack or presence on an IS where the virus has executed on that system.
- **Vulnerability.** Any detected lack of protection which may render the system vulnerable to security breaches. Examples are: failure, or potential failure, of a system or network security feature; the discovery of any computer code, such as a trapdoor, which was originally coded into the operating system by the software vendor; or code added by software maintenance personnel, that provides an undocumented entry/exit capability into the system by unauthorized personnel.

8.3.3. (U) Reporting Incidents. Incidents in progress are classified a minimum of CONFIDENTIAL in accordance with NSA/CSS Classification Guide 75-98 or DoD 5105.21-M-1. The cognizant intelligence agency (DIA or NSA) should be notified by electrical message (AUTODIN) or E-Mail as soon as the unit has knowledge of an incident or specifics. The notification should contain the information in paragraph 8.3.4.

(see Figure 8.1 for an example of an AUTODIN message). Initial/interim reporting should begin as soon as possible after knowledge of the incident, but should continue until the incident is resolved. You may also communicate to the agencies by secure telephone, or use the Web-based forms on the DIA or NSA web sites. Remember to include information copies of the report to the DAA Rep/SCO and chain of command (for example, AIA, INSCOM, SSO NAVY, CNSG). Complete the report according to the format in paragraph 8.3.4 below and send to the appropriate Service addressees. SCEs will report to the Security Health Officer (SHO) desk in the NSA/CSS IS Incident Response Team (NISIRT), phone: DSN 644-6988/Commercial (301) 688-6988. DoDIIS sites will report to the DIA ADP Command Center, phone: DSN 428-8000/Commercial (202) 231-8000. For guest systems, reporting should be to both the cognizant SCIF authority and the guest system DAA Rep/SCO. Do not report as incidents, users playing games on the systems, or fraud waste and abuse issues, unless they constitute a threat to the security of a system. This type of incident should be reported and dealt with by the unit's chain of command.

8.3.4. (U) Report Format and Content. When reporting incidents, include the following information in the body of the message (as shown in sample message, Figure 8.1):

- **Type of Incident.** Enter the type of incident report directly from paragraph 8.3.2 above. If there is any doubt when choosing the "type" of incident, identify the incident as both (or multiple) types in the same message. Selecting the most appropriate incident type is not nearly as important as reporting the incident.
- **Date and Time the Incident Occurred.** Enter the date and time that the occurrence was first detected.
- **Name and Classification of the Subject IS.** Enter the name of the system identified in the accreditation documentation, a current description of the hardware and software on the system, and the highest classification of information processed.
- **Description of the Incident.** Clearly describe the incident in detail.
- **Impact of the Incident on Organization Operations.** This is usually stated in terms of "denial of service", such as having to isolate the IS from a network, thereby closing down operations, etc. Include the number of hours of system downtime and how many man-hours needed to correct the problem.
- **Impact of the Incident on National Security.** Per DoD 5105.21-M-1, when classified information has been released to unauthorized persons, you must treat the incident as a security violation. List the name of the SCI security official to whom you have reported the incident.
- **Man-hours involved in recovery, cleanup, etc.** This provides an accurate metric to track incident recovery man-hours and resources involved. Tracking can include cost estimates related to the hours/wage grade spent.
- **Point Of Contact (POC).** Enter the name, rank, organization, office, and telephone number of the person to be contacted on all subsequent actions concerning this incident.

R 211234Z FEB 01

FM *YOUR UNIT*//OFFICE//

TO SSO DIA//SYS-4/DAC-3D//

NSACSS//SHO/L1//

INFO *CHAIN OF COMMAND*

***SCO*//OFFICE//**

ZEM

C O N F I D E N T I A L

QQQQ

SUBJECT: INCIDENT REPORT ICW JDCSISSS, CHAPTER 8

1. TYPE OF INCIDENT: (VIRUS, MALICIOUS CODE, DATA COMPROMISE, SUSPECTED PROBLEM)

2. DATE/TIME INCIDENT OCCURRED

3. NAME AND CLASSIFICATION OF VICTIMIZED SYSTEM

4. DESCRIPTION OF INCIDENT: (AS MUCH DETAIL AS NECESSARY TO ADEQUATELY DESCRIBE THE PROBLEM)

5. IMPACT OF INCIDENT ON ORGANIZATION OPERATIONS (USUALLY STATED IN TERMS OF DENIAL OF SERVICE, DOWN TIME OR MISSION IMPACT)

6. IMPACT OF THE INCIDENT ON NATIONAL SECURITY (USUALLY STATED IN TERMS OF DATA OWNER'S ASSESSMENT OF LEVEL OF CLASSIFIED INFORMATION AND COMPROMISE PROBABILITY)

7. MAN-HOURS REQUIRED TO COMPLETE RECOVERY

8. ACTIONS TAKEN TO RECOVER

9. REPORTING UNIT POC (NAME, RANK, ORG/OFFICE, PHONE NUMBERS, E-MAIL ADDRESS)

NNNN

Figure 8.1 (U) Sample Incident Report Message

8.3.5. (U) Follow-On Action. Units will continue to report until the incident is closed. Virus infections that are corrected should be reported as "closed", unless further actions are being taken, or reinfection has occurred. Follow-on actions will be determined by the HQ-level action addressees and Data Owners. Appropriate PAA/designee will determine course of action for incident cleanup in a near real-time manner. Once an incident has been resolved (i.e., closed), the incident may be treated as FOUO. The Designated Approving Authority (DAA) Representative (Rep)/SCO will coordinate with the Defense Intelligence Agency (DIA) or National Security Agency/Central Security Service (NSA/CSS) Information Systems Incident Response Team (NISIRT) to ensure that the concerns of the latter are addressed. If an activity from another command or agency is involved, the HQ-level action addressees will provide proper notification to the same.

CHAPTER 9

INFORMATION SYSTEM (IS) MONITORING ACTIVITIES

9.1. (U) PURPOSE. This chapter provides guidance on the DOs and DON'Ts of IS monitoring and applies to all computer systems and networks. All U.S. Government systems must be protected from everything from exploitation by adversaries to intrusion by inquisitive hackers. Therefore, it is mandatory this guidance be implemented whether or not "keystroke monitoring" is being conducted. Incidents of unauthorized intrusion are an annoyance, if not catastrophic, depending upon the circumstances. Intrusions may result in denial of service, misuse, destruction and modification of data or programs, and disclosure of information. Typically, the personnel and physical security disciplines add credence to the protection afforded Government systems, especially those that are classified. Occasionally, when the incident requires further action, some monitoring must be established as an additional tool to protect the critical system and to identify the perpetrator attempting to violate the security of the system.

9.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

9.3. (U) PROCEDURES. In the DoD environment, the policy is to protect classified and unclassified sensitive information from unauthorized disclosure, destruction and modification. The security policies have been constructed to meet this objective. Implementation of these security policies begins with a warning to the user that the system is subject to monitoring. Once this has been done, the user acknowledges that some line monitoring or keystroke monitoring may be initiated when appropriately authorized and determined necessary to provide documentary evidence for a potential prosecution or administrative action. Extreme care must be taken in a targeted monitoring situation, in accordance with (IAW) this Chapter, to ensure:

- Evidence is not destroyed.
- Innocent personnel are not implicated.
- The subject does not become aware of a planned monitoring activity.

9.3.1. (U) IS Warning Banner. The Department of Defense (DoD) General Counsel has advised that managers of Federal Systems who conduct "keystroke monitoring" to protect their systems and networks from unauthorized access, should provide explicit notice to all users that use of these systems constitutes consent to monitoring. User knowledge of monitoring activation can serve as a deterrent to any malicious act.

9.3.1.1. (U) A logon warning banner is required on all networked and standalone DoD interest computer systems (Government and contractor). The warning banner must be displayed before a successful logon and should include an option that allows the user to halt the logon process. The intent of the banner is to confirm to the user that all data contained on DoD interest computer systems is subject to review by law enforcement authorities, DoD security personnel, and/or System Administrator, IAW this chapter. The banner is designed to inform all users, prior to accessing a DoD system, that by logging on they expressly consent to authorized monitoring.

9.3.1.2. (U) ISs supporting DoD operations have very specific warning banner requirements, and must include, at a minimum, the information shown in Figure 9.1.

9.3.1.3. (U) A warning banner must be placed on an IS so that the IS user must enter a keystroke to continue processing. Although an appropriate warning banner is displayed, systems administration personnel will minimize the possibility of accessing user data that is not relevant to the monitoring being acquired, analyzed, or recorded. Whenever system administration personnel suspect that a system is being inappropriately used, either by authorized or unauthorized personnel, or some improper activity is being conducted, the matter will be reported immediately to the Information Systems Security Manager (ISSM). Any monitoring directed at specific individuals suspected of unauthorized activity must be authorized by local authority/General Counsel and coordinated with the Designated Approving Authority (DAA)/DAA Rep/Service Certifying Organization (SCO) (see paragraph 9.3.3).

NOTICE AND CONSENT BANNER

THIS IS A DEPARTMENT OF DEFENSE (DOD) COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM,

TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.

USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

FIGURE 9.1. (U) INFORMATION SYSTEM WARNING BANNER.

9.3.2. (U) Warning Labels. In addition to the IS warning banner, a standard U.S. Government warning label must be placed on the top border edge of each terminal of each IS. Local production of labels is authorized only when using the text contained in Figure 9.2.

THIS AUTOMATED INFORMATION SYSTEM (AIS) IS SUBJECT TO MONITORING AT ALL TIMES. USE OF THIS AIS CONSTITUTES CONSENT TO MONITORING.

FIGURE 9.2. (U) WARNING LABEL.

9.3.3. (U) Action To Be Taken In A Monitoring Incident. When monitoring is justified and approved, the ISSM and Information System Security Officer (ISSO)/System Administrator (SA), in conjunction with the DAA/DAA Rep/SCO, should take every effort to ensure that the actions identified in Table 9.1 are performed in an orderly fashion. For additional information on monitoring see 7.4.10.

*****CAUTION*****

Do not proceed to monitor an individual without first gaining permission and guidance from General Counsel and Commander/CO/SIO. Unauthorized targeted monitoring is a violation of the subject's rights and may jeopardize the investigation. Authorization for targeted monitoring must come through the Commander/Commanding Officer in consultation with legal representation -- Judge Advocate General (JAG), General Counsel, or authorized investigative organization (Defense Criminal Investigative Service (DCIS), US Army Criminal Intelligence Department (USACID), US Army Military Intelligence (USAMI), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI)). The ISSM and ISSO/SA will make every effort to answer all applicable questions identified in Table 9.2.

9.3.4. (U) Review System Specific Security Features. The investigators will want full documentation on many aspects of the system being violated. Table 9.2 identifies sample information needed by the Commander/CO/SIO which may be needed in justifying the investigation. The ISSM and ISSO/SA will make every effort to document the information in Table 9.2.

TABLE 9.1. (U) RECOMMENDED INCIDENT RESPONSE ACTIONS

ITEM NUMBER	ACTION RECOMMENDED
1	Notify the ISSM.
2	The ISSM will notify the Special Security Officer (SSO), Commander/CO/SIO
3	The Commander/CO/SIO will coordinate with the General Counsel and authorized investigative office for formal guidance.
4	Follow Chapter 8 for incident reporting
5	Keep a record of actions by the ISSM concerning the incident.

TABLE 9.2. (U) SAMPLE MONITORING INVESTIGATION QUESTIONS

ITEM NUMBER	SAMPLE INFORMATION THAT MAY BE NEEDED BY THE COMMANDER
1	What event(s) triggered suspicion of improper system use?
2	Does the system have a warning banner? Is the banner displayed prior to the first keystroke?
3	Where is the hardware physically located?
4	What level of classified data is processed on the system?
5	What organization/activity is supported by the system?
6	What connectivities are authorized to the system?
7	What is the function of the system?
8	What security software, if any, is used on the system?
9	Are audit trails running normally and have they been reviewed regularly?
10	Is a copy of the SSAA/SSP available?

CHAPTER 10

MALICIOUS CODE PREVENTION

10.1. (U) PURPOSE. Minimize the risk of malicious code (malicious logic) from being imported to or exported from Information Systems (ISs). Preventing malicious code is everyone's responsibility. This chapter identifies various types of malicious code and provides preventive measures to avoid problems.

10.2. (U) SCOPE. The provisions of this policy applies to all organizations processing Sensitive Compartmented Information (SCI), their components, and affiliates worldwide, as well as all contractor-owned or operated systems employed in support of SCI designated contracts. This supplement will be specified on all DD Forms 254 as a contractual requirement. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

10.3. (U) DEFINITIONS.

10.3.1. (U) Malicious code. Malicious code is that which is intentionally included in hardware, software, firmware or data for unauthorized purposes. Computer Viruses, Worms, Trojan Horses, Trapdoors, and Logic/Time Bombs all fall under the definition of malicious code. Computer viruses pose the primary threat to ISs because of their reproductive capability. Malicious code can arrive through either media that are introduced to ISs or as mobile code that arrives through connections to other systems and networks.

10.3.2. (U) Mobile Code. Mobile code is technology which allows for the creation of executable information which can be delivered to an information system and then directly executed on any hardware/software architecture which has an appropriate host execution environment. The code can perform positive or negative actions (malicious). The focus on risk is based on the receipt of executable information from sources outside a Designated Approval Authority's area of responsibility or control. Mobile code is the software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.

10.3.3. (U) Malicious Mobile Code. Mobile code is the software designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources. Types of mobile code are direct and indirect.

- Direct mobile code can be recognized within the primary transport mechanism, such as a virus within a file.
- Indirect mobile code may be embedded, such as inside of an attachment to an E-Mail.

10.3.4. (U) Mobile Code Technologies. Software technologies that provide the mechanisms for the production and use of mobile code are grouped into three Risk Categories based on the functions performed by the code, the ability to control distribution of the code and control of the code during execution.

10.3.4.1. (U) Category 1 is mobile code that can exhibit broad functionality using unmediated access to services and resources of workstations, hosts and remote systems. Category 1 mobile code technologies can pose severe threats to IC services. Some of these technologies allow differentiation between unsigned and signed code (i.e., a mechanism used by a trusted source), with capabilities to configure systems so that only signed code will execute. Examples of Category 1 technologies include:

- Active X;
- Visual Basic for Applications (VBA);
- Windows Scripting Host, when used as mobile code;
- Unix Shell scripts, when used as mobile code; and
- MS-DOS Batch Scripts, when used as mobile code.

10.3.4.2. (U) Category 2 is mobile code that has full functionality using mediated or controlled access to services and resources of workstations, hosts and remote systems. Category 2 mobile code technologies may employ known and documented fine-grain, periodic, or continuous countermeasures or safeguards against malicious use. Some of these technologies allow differentiation between unsigned and signed code (i.e., a mechanism used by a trusted source), with capabilities to configure systems so that only signed code will execute. Examples of Category 2 technologies include:

- Java Applets and other Java Mobile Code;
- LotusScript;
- PerfectScript; and
- Postscript.

10.3.4.3. (U) Category 3 is mobile code that has limited functionality, with no capability for unmediated or uncontrolled access to services and resources of workstations, hosts and remote systems. Category 3 mobile code technologies may employ known and documented fine-grain, periodic, or continuous countermeasures or safeguards against malicious use. Protection against these types of mobile only requires normal vigilance compared with that required to keep any software configured to resist known exploits. Examples of Category 3 technologies include:

- JavaScript (includes Jscript and ECMAScript variants);
- VBScript;
- PortableDocumentFormat (PDF); and
- Shockwave/Flash.

10.3.4.4. (U) Exempt technologies are those which are not considered true mobile code. These include:

- XML;
- SMIL;
- QuickTime;
- VRML (exclusive of any associated Java Applets or JavaScript Scripts);
- Web server scripts, links and applets that execute on a server (Java servlets, Java Server Pages, CGI, Active Server Pages, CFML, PHP, SSI, server-side JavaScript, server-side Lotus Script);
- Local programs and command scripts that exist on a user workstation (binary executables, shell scripts, batch scripts, Windows Scripting Host (WSH), PERL scripts);
- Distributed object-oriented programming systems that do not go back to the server to execute objects (CORBA, DCOM); and
- Software patches, updates and self-extracting updates that must be explicitly invoked by a user (Netscape SmartUpdate, Microsoft Windows Update, Netscape web browser plug-ins, and Linux Update Manager)

10.3.5. (U) Trusted Source. A trusted source is a source that is adjudged to provide reliable software code or information and whose identity can be verified by authentication. The following mechanisms are sufficient to validate the identity of a trusted source:

- a connection via JWICS;
- a connection via the SIPRNET;
- a digital signature over the mobile code itself using either DoD or IC-approved PKI certificate;
- a commercial certificate approved by either the DoD CIO or the IC CIO; or
- authentication of the source of the transfer by public key certificate (e.g., S/MIME, SSL server certificate from an SSL web server).

10.3.6. (U) Screening. Screening is a preventive measure to monitor processes and data to intercept malicious code before it is introduced to an IS. Screening also includes monitoring IS for the presence of malicious code which is already present. Malicious code occurs in different forms, which may have different methods for screening.

10.4. (U) PROCEDURES. The ISSM/ISSO is responsible for ensuring that the following procedures are followed:

10.4.1. (U) Preventive Procedures. Scan all information storage media (e.g., diskettes, compact disks, computer hard drives, etc.) and E-mail attachments introduced prior to its use on any SCI system. If the media cannot be scanned then it is considered high risk and cannot be used on any SCI system without approval from the Service Certifying Organization (SCO). Procedures to be followed:

- Use automated scanning applications, e.g., virus scanning, which will monitor media upon introduction to a system and data being transferred into the IS.
- Check and review the IS operating environment for the presence of malicious code on a frequent basis.
- Avoid hostile mobile code through use of only authorized/verified and registered mobile code.
- Keep automated scanning processes up to date with the most current recognition signatures.
- Ensure that users will not knowingly or willfully introduce malicious code into systems.
- Ensure that users will not import or use unauthorized data, media, software, firmware, or hardware on systems.
- Ensure that users will conduct screening of all incoming data (e.g., E-Mail and attachments) if this process is not automated.
- Ensure that users will not use personal-owned media (e.g., music, video, or multimedia compact disks) in Government-owned IS.
- Ensure that all users immediately report all security incidents and potential threats and vulnerabilities involving malicious code on ISs to the ISSM.
- Controlled Interfaces with malicious code scanning capability does not relieve the management of the receiving IS from the responsibility of also checking for malicious code.

10.4.2. (U) Malicious Code Detection. If a malicious code is detected or a presence of malicious code is suspected on any IS, do the following:

- Immediately report it to the ISSM for further instruction in accordance with Chapter 8. Do nothing that might cause the further spread of the malicious code.
- Take the following corrective actions:
  - If found in a file, use approved Anti-virus software to remove a virus from a file.
  - If found on a System, use approved Antivirus software to remove the virus from your system.
  - If files are corrupted, then restore affected files from system backups.

10.5. (U) MALICIOUS CODE SECURITY REQUIREMENTS. An integral part of this program is the mandatory training required by public law. Users shall receive initial training on prescribed IS security restrictions and safeguards prior to accessing corporate IS assets in accordance with Chapter 6. User awareness is still the first line of defense, especially since there is NO ANTI-VIRUS SOFTWARE THAT CAN GUARANTEE 100% PROTECTION FROM VIRUSES.

10.5.1. (U) Preventative Steps to be Taken:

- Employ user awareness education.
- Use virus scanning programs to detect viruses that have been placed on diskettes.
- Never start a PC while a diskette is in the drive.
- Ensure the CMOS boot-up sequence for PCs is configured to boot-up from the hard drive first (usually the C: drive) NOT the A: drive.
- Block receiving/sending of executable code. Blocking files with executable extensions such as EXE, VBS, SHS etc., contributes to overall anti-virus measures.
- Adopt procedures to configure email applications to view received files/attachments in a "viewer." Viewers normally do not have macro capabilities.
- Avoid using a diskette from an outside source without first scanning it for potential viruses.
- Avoid downloading data from internet bulletin boards, etc., unless the file can be scanned for viruses beforehand.
- Ensure files are being backed up daily.
- Implement a process to routinely check security bulletins for updates, (i.e., CERT, AFCERT, NAVCERT, etc.)
- Whenever possible, disable the automatic execution of all categories of mobile code in email bodies and attachments.
- Whenever possible, desktop software shall be configured to prompt the user prior to opening email attachments that may contain mobile code.

CHAPTER 11

SOFTWARE

11.1. (U) PURPOSE. This chapter defines the various types of software applications that may be used on any DoD IS. It lists software types that are authorized as well as specific types of software that are not authorized.

11.2. (U) DEFINITION. For the purpose of this policy, software should be interpreted to be any information recorded on any information storage media to include data files, source code and executable code.

11.3. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

11.4. (U) PROCEDURES FOR SOFTWARE AUTHORIZATION. Additions or modifications to software on systems which affects system accreditation must be evaluated by the ISSM through the local Configuration Management Board/Configuration Control Board (CMB/CCB) process and coordinated with the DAA Rep/SCO to gain concurrence. The provisions of this policy apply to all organizations processing Sensitive Compartmented Information (SCI), their components, and affiliates worldwide.

11.5. (U) LOW RISK SOFTWARE. Low risk software may be introduced on SCI ISs, to include stand-alone personal computers. Low risk - authorized software must be approved by the ISSPM/ISSM and includes the following:

11.5.1. (U) Provided officially by another U.S. Government Agency that has equivalent standards.

11.5.2. (U) Provided under contract to organizations involved with the processing of SCI and related intelligence information.

11.5.3. (U) Developed within a Government-approved facility.

11.5.4. (U) Commercial Off-The-Shelf (COTS) software provided through appropriate procurement channels.

11.5.5. (U) Distributed through official channels.

11.5.6. (U) Acquired from a reputable vendor for official use or evaluation (i.e., maintenance diagnostic software).

NOTE: In all cases, system and site specific security policy should be considered.

11.6. (U) HIGH RISK SOFTWARE. Certain software is deemed "high risk" and is not authorized for use without approval. Such software must be approved in writing by the respective DAA Rep/SCO before it may be legally used. High risk software includes public domain, demonstration software, and embedded software not obtained through official channels. Other software may be deemed high risk by the DAA Rep/SCO.

11.6.1. (U) Public Domain Software. Only the DAA (Rep)/SCO may approve the use of public-domain software. Do not confuse public-domain software with off-the-shelf, or user developed software. A request to use public-domain software and the subsequent approval requires an extensive evaluation, by approved evaluation centers, of the particular software source code in search of Trojan Horses, Trapdoors, Viruses, etc. There is limited capability to perform these required evaluations.

11.6.2. (U) Demonstration Software and Media. Floppy diskettes and removable hard disks used for demonstrations, with the intent of being returned to a vendor, must be processed on a computer that has never processed or stored classified data. Otherwise, the demonstration media cannot be released back to the vendor and should be destroyed. If it is to be returned to the vendor, a fully cleared and indoctrinated individual must verify that the media was used only in an unclassified computer.

11.6.3. (U) Embedded Software. Game software included as part of a vendor bundled software or software/hardware package shall be removed from the IS immediately following the installation and testing of the software. Vendor supplied games occupy valuable disk space and could open the door for Fraud, Waste, and Abuse (FW&A) charges. Game software provided for use as tutorials may be granted as an exception to this restriction by the DAA Rep/SCO. All other games software currently on SCI ISs are considered a violation of this policy and must be removed.

11.6.4. (U) Unauthorized Software. Types of software that are not authorized include:

- Games (See paragraph 11.6).
- Public domain software or "shareware" which have been obtained from unofficial channels.
- All software applications which have been developed outside Government approved facilities, such as those developed on personally owned computers at home or software acquired via non- U.S. Government "bulletin boards".
- Personally owned software (either purchased or gratuitously acquired).
- Software purchased using employee funds (from an activity such as a coffee fund).
- Software from unknown sources.
- Illegally copied software in violation of copyright rules.
- Music and video or multimedia compact disks, not procured through official Government channels.

11.6.5. (U) IA Software and Security Tools. Some high risk software may be required to meet system requirements. For example, to comply with paragraph 4.B.2.a.5.b of DCID 6/3, intrusion/attack detection and monitoring tools are required to support required periodic testing by the ISSO/ISSM within their domain.

CHAPTER 12

INFORMATION STORAGE MEDIA CONTROL AND ACCOUNTING PROCEDURES

12.1. (U) PURPOSE. This chapter outlines the minimum requirements for the control and accounting of information storage media. The Commander/Commanding Officer is responsible to prescribe the policy for the level of control and accounting appropriate for information storage media under his/her control.

12.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

12.3. (U) PROCEDURES. This chapter provides guidelines for control and accounting of information storage media. For any system that operates with PL-3 or lower functionality, media which is not write-protected and is placed into that system must be classified at the highest level of information on the system until reviewed and validated. Media accountability will be based on the determined classification level of the media.

12.3.1. (U) Information Storage Media Control. In addition to the labeling of information storage media IAW Chapter 13, there is a requirement to control and account for certain information storage media within functional categories. This chapter tasks the organization Commander/Commanding Officer with developing a unit-unique Standard Operating Procedure (SOP) for control and accountability.

12.3.1.1. (U) Inspections. The organization must be able to demonstrate positive control and accounting of information storage media according to its SOP when being inspected by authorities.

12.3.1.2. (U) Control Procedures. Control of information storage media should begin upon introduction into the organization according to the SOP.

12.3.1.2.1. (U) Information storage media accountability is required for Top Secret BRAVO and permanent Collateral Top Secret files.

12.3.1.2.2. (U) Information storage accountability as a security protection measure is eliminated for collateral classified information (to include Top Secret non-permanent files), all classification levels of Special Intelligence (SI) (to include GAMMA and ENDSEAL), Talent-Keyhole (TK), and BRAVO material below Top Secret.

12.3.1.2.3. (U) Requirements for control of specific Special Access Program (SAP) information will be communicated by the respective Program Manager.

12.3.1.3 (U) Other Categories of Storage Media. The following major categories of information storage media should be considered for accountability in compliance with copyright and licensing as documented in the SOP:

- Commercial Off-The-Shelf (COTS) and vendor software.
- Government developed software.
- Other organization unique software and data.

12.3.2. (U) Audits and Reports. Each organization will periodically audit the information storage media accountability records for accuracy. The frequency of audits should depend on the volume of media on hand, the frequency of changes in the accounting system, criticality of the media, and classification level of data stored onto the media. Perform other audits at the Commander's/Commanding Officer's discretion. Document the result of these audits in an internal report to remain on file within the organization for at least one year. Report discrepancies to the ISSM for further reporting to the DAA Rep/SCO as required. These requirements should be addressed in the organization SOP.

12.3.2.1. (U) Inventories/audits will be required for accountable information storage media described in paragraph 12.3.1.2. Information storage media holdings will be audited periodically to ensure proper control is being maintained and media is destroyed when no longer needed.

12.3.2.2. (U) Barcodes will only be assigned to accountable material described in paragraph 12.3.1.2.

12.3.3. (U) Destruction of Media. When destruction of information storage media is appropriate and approved, it must be accomplished according to approved procedures and methods and an update to the organization media accounting system should be made. See Chapter 20, Paragraph 20.4.5, Destroying Media, for additional guidance.

12.3.3.1. (U) Destruction certificates are required for accountable material and will be retained as a permanent record.

12.3.3.2. (U) Non-accountable material no longer requires destruction certificates.

CHAPTER 13

INFORMATION STORAGE MEDIA LABELING AND PRODUCT MARKING REQUIREMENTS

13.1. (U) PURPOSE. This chapter outlines the minimum requirements for marking the magnetic media and paper products. Labeling of magnetic media is similar to labeling paper products. Like paper documents, all information storage media must be properly marked with the appropriate classification and handling instructions.

13.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

13.3. (U) PROCEDURES. To ensure data integrity and protection, information storage media must be administratively labeled and appropriately protected to prevent the loss of information through poor security practices. Likewise, to prevent security compromises, all output products must be appropriately protected. Proper classification marking of output paper products, microfiche, terminal screen displays and central processing units (CPUs) must be accomplished and is the responsibility of the user. Each supervisor is ultimately responsible for the labeling, handling, and storage of both media and paper products within their assigned area of responsibility.

13.3.1. (U) Information Storage Media. Removable IS storage media and devices shall have external labels clearly indicating the classification of the information and applicable associated markings (e.g., digraphs, trigraphs). Labeling exemption for operational security (OPSEC) requirements may be granted within local policy with DAA/DAA Rep/SCO concurrence. Examples include magnetic tape reels, cartridges, cassettes; removable discs, disc cartridges, disc packs, diskettes, magnetic cards and electro-optical (e.g., CD) media. All removable information storage media and devices will be marked with the appropriate Standard Form (SF) 700-series classification and descriptor labels. These are:

- SF 706, Top Secret Label (Collateral only)
- SF 707, Secret Label (Collateral only)
- SF 708, Confidential Label (Collateral only)
- SF 710, Unclassified Label
- SF 711, Data Descriptor (On all magnetic media)
- SF 712, Classified SCI Label (All classification levels)

13.3.1.1. (U) Label Placement. See the Federal Register 2003 and applicable military department regulations for exact placement procedures. Labels will be affixed to all media in a manner that does not adversely affect operation of the equipment in which the media is used. Labels may be trimmed to fit the media. Labels for Compact Disks (CDs) must NOT be placed on the CD itself. Place the labels on the CD container or envelope. Record the accounting number in the "Control" block of the SF 711 and write the same number on the CD with a Paint-pen, CD labelmaker or permanent marker. The number should not interfere with the operation of the CD. Notice: Do not use pens that contain toluene.

13.3.1.2. (U) Data Descriptor Label. The SF 711, Data Descriptor Label, identifies the content of a specific media to include unclassified, collateral-classified, and Sensitive Compartmented Information (SCI). An SF 711 is not required if the disk bears the following information: Organization, office symbol, classification, and media sequence number (if locally required). The user fills in the "Classification", "Dissem",

"Control", and "Compartments/Codewords" blocks as appropriate.

13.3.2. (U) Classification Markings. All documents residing or processed on information storage media/ISs will be marked in accordance with Department of Defense (DoD) 5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual, or appropriate Service regulations.

CHAPTER 14

INFORMATION SYSTEMS (IS) MAINTENANCE PROCEDURES

14.1. (U) PURPOSE. The purpose of this chapter is to identify security procedures and responsibilities which must be followed during the maintenance of Information Systems (IS). ISs are particularly vulnerable to security threats during maintenance activities. The level of risk is directly associated with the maintenance person's clearance status (cleared or uncleared). A maintenance person may be uncleared or may not be cleared to the level of classified information contained on the IS. Properly cleared personnel working in the area must maintain a high level of security awareness at all times during IS maintenance activities. Additionally, the Information Systems Security Manager (ISSM) is responsible for IS maintenance security policy, including maintenance procedures for all ISs under his or her control.

14.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

14.3. (U) PROCEDURES:

14.3.1. (U) Maintenance Personnel:

14.3.1.1. (U) Maintenance by Cleared Personnel. Personnel who perform maintenance on classified systems should be cleared and indoctrinated to the highest classification level of information processed on the system. Appropriately cleared personnel who perform maintenance or diagnostics on ISs do not require an escort. However, an appropriately cleared and, when possible, technically-knowledgeable employee should be present when maintenance is being performed to assure that the proper security procedures are being followed.

14.3.1.2. (U) Maintenance by Uncleared (or Lower-Cleared) Personnel. If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used provided a fully cleared and technically qualified escort monitors and records their activities in a maintenance log.

14.3.1.2.1. (U) Uncleared maintenance personnel should be US citizens. Outside the US, where US citizens are not available to perform maintenance, foreign nationals may be utilized, but only with Designated Approving Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO) approval.

14.3.1.2.2. (U) Prior to maintenance by uncleared personnel, the IS will be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured. When a system cannot be cleared, ISSM-approved procedures will be enforced to deny the uncleared individual visual and electronic access to any classified or sensitive data that is contained on the system.

14.3.1.2.3. (U) A separate, unclassified copy of the operating system (e.g., a specific copy other than the copy(s) used in processing information), including any floppy disks or cassettes that are integral to the operating system, will be used for all maintenance operations performed by uncleared personnel. The copy will be labeled "UNCLASSIFIED--FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSAA/SSP. Maintenance procedures for an IS using a non-removable storage device on which the operating system is resident will be considered and approved by the ISSM on a case-by-case basis.

14.3.2. (U) General Maintenance Requirements:

14.3.2.1. (U) Maintenance Log. A maintenance log must be maintained for the life of the IS. The maintenance log should include the date and time of maintenance, name of the individual performing the maintenance, name of escort, and a description of the type of maintenance performed, to include identification of replacement parts. Maintain this log for the life of the IS.

14.3.2.2. (U) Location of Maintenance. Maintenance should be performed on-site whenever possible. Equipment repaired off-site and intended for reintroduction into a Sensitive Compartmented Information Facility (SCIF) may require protection from association with that particular SCIF or program.

14.3.2.3. (U) Removal of Systems/Components. If systems or system components must be removed from the SCIF for repair, they must first be purged, and downgraded to the appropriate classification level, or sanitized of all classified data and declassified IAW ISSM-approved procedures. The ISSM, or designee, must approve the release of all systems and parts removed from the system.

14.3.2.4. (U) Use of Network Analyzers. Introduction of network analyzers that provide maintenance personnel with a capability to do keystroke monitoring must be approved by the ISSM, or designee, prior to being introduced into an IS. See Chapter 9, Paragraph 9.3.3, for additional guidance.

14.3.2.5. (U) Use of Diagnostics. If maintenance personnel bring diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics) into a SCIF, the media containing the programs must be checked for malicious codes before the media is connected to the system, must remain within the SCIF, and must be stored and controlled at the classification level of the IS. Prior to entering the SCIF, maintenance personnel must be advised that they will not be allowed to remove media from the SCIF. If deviation from this procedure is required under special circumstances, then each time the diagnostic test media is introduced into a SCIF it must undergo stringent integrity checks (e.g., virus scanning, checksum, etc.) prior to being used on the IS and, before leaving the facility, the media must be checked to assure that no classified information has been written on it. Such a deviation must be approved by the ISSM.

14.3.2.6. (U) Introduction of Maintenance Equipment into a SCIF. All diagnostic equipment or other items/devices carried into a SCIF by maintenance personnel will be handled as follows:

14.3.2.6.1. (U) Systems and system components being brought into the SCIF shall, as far as practical, be inspected for improper modification.

14.3.2.6.2. (U) Maintenance equipment that has the capability of retaining information must be appropriately sanitized by established procedures (see Chapter 13) before being released. If the equipment cannot be sanitized, it must remain within the facility, be destroyed, or be released under procedures approved by the DAA Rep/SCO.

14.3.2.6.3. (U) Replacement equipment or components that are brought into the SCIF for the purpose of swapping-out facility components are allowed. However, any component introduced into an IS will remain in the facility until proper release procedures are completed.

14.3.2.6.4. (U) Communication devices with transmit capability (e.g., pagers, RF LAN connections, etc.) and any data storage device not essential to maintenance, shall remain outside the SCIF.

14.3.3. (U) Maintenance and System Security. After maintenance, and before return to operation, the ISSM, or designee, shall check the security features on the IS to assure that they still function properly. Additionally, any maintenance changes that impact the security of the system shall receive a configuration management review.

14.3.4. (U) Remote Maintenance:

14.3.4.1. (U) Requirements/Considerations:

14.3.4.1.1. (U) The Installation and use of remote diagnostic links must be preapproved and procedures addressed in the SSAA/SSP.

14.3.4.1.2. (U) An audit log shall be maintained for five years of all remote maintenance, diagnostic, and service transactions and periodically reviewed by the Information System Security Officer (ISSO)/System Administrator (SA).

14.3.4.1.3. (U) Other techniques to consider when remote maintenance is required include encryption and decryption of diagnostic communications, strong identification and authentication techniques such as tokens, and remote disconnect verification.

14.3.4.2. (U) Maintenance Performed with the same Level of Security. Remote Diagnostic Maintenance service may be provided by a service or organization that does possess the same level and category(ies) of security. The communications links connecting the components of the systems, plus associated data communications and networks, shall be protected in accordance with national security policies and procedures applicable to the sensitivity level of the data being transmitted.

14.3.4.3. (U) Maintenance Performed with a different Level of Security. If remote diagnostic or maintenance services are required from a service or organization that does not provide the same level of security required for the IS being maintained, the system must be cleared; placed in a standalone configuration prior to the connection of the remote access line; and maintenance personnel must possess the appropriate clearance to perform the maintenance. If the system cannot be cleared (e.g., due to a system crash), remote diagnostics and maintenance shall not be allowed.

14.3.4.4. (U) Initiating and Terminating Remote Access. The initiation and termination of the remote access must be performed by the ISSM or designee.

14.3.4.5. (U) Keystroke Monitoring Requirements. Keystroke monitoring shall be performed on all remote diagnostic or maintenance services. So far as practicable, a technically qualified person shall review the maintenance log to assure the detection of unauthorized changes. The ISSM, or designee, will assure that maintenance technicians responsible for performing remote diagnosis/maintenance are advised (contractually, verbally, banner, etc.) prior to remote diagnostics/maintenance that keystroke monitoring will be performed.

14.3.5. (U) Life Cycle Maintenance. The requirement for, and vulnerabilities of, IS maintenance, whether performed by military or contractor personnel, must be addressed during all phases of the system's life cycle. The security implications of IS maintenance must be specifically addressed when entering into contract negotiations for any maintenance activity.

CHAPTER 15

PORTABLE ELECTRONIC DEVICES

15.1. (U) PURPOSE. This chapter identifies procedures for the entry and exit of portable electronic devices into SCIFs. A portable electronic device is a generic term used to describe the myriad of small electronic items that are widely available. The rapid growth in technological capabilities of portable electronic devices/portable computing devices (PEDs/PCDs) has led to concerns about their portability into and out of Sensitive Compartmented Information Facilities (SCIFs). PEDs include cellular telephones, two way pagers, palm sized computing devices, two-way radios, audio/video/data recording, playback features, personal digital assistants, palm tops, laptops, notebooks, data diaries, and watches with communications software and synchronization hardware, that may be used to telecommunicate. These devices must be closely monitored to ensure effective control and protection of all information on our IS.

15.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

15.3. (U) RISK. Because PEDs are designed to freely and openly exchange information, most users may not be aware of the technologies that reside in the various PEDs. PEDs may contain wireless or infrared capabilities. Thus, users do not always know when automated information transfer is active or that the PED is being reprogrammed or reconfigured remotely without their knowledge

15.3.1. (U) Classified Information. The introduction of unauthorized classified information to a PED, will result in a security violation (see Chapter 8). For example: aggregation of data, inadvertent wireless connection, and POCs maintained through classified or sensitive contracting mechanisms. If this occurs to an unclassified PED, the PED needs to be controlled as classified material (e.g., this could include confiscation of the PED). If a PED is already classified, and unauthorized classified information is found (higher than authorized for the PED), the PED needs to be controlled at the higher, more restrictive level.

15.4. (U) PROCEDURES. The use of PEDs in a SCI environment presents a high degree of risk for the compromise of classified or sensitive information. PEDs will only be used to fulfill mission requirements. Additionally, very specific handling procedures must be developed and made available to the user of the PED. The Agency in charge of any given SCIF is the authority for the procedures to move PEDs in or out of their facilities. Specific requirements/procedures are:

15.4.1. (U) Approval Requirements. All of the following requirements must be satisfied prior to approving the use of portable electronic devices:

15.4.1.1. (U) Personal PEDs

- Personal PEDs, hardware/software associated with them, and media are prohibited from entering/exiting a SCIF unless authorized by the Agency granting SCIF accreditation.
- Personal PEDs are prohibited from operating within a SCIF unless authorized by the agency granting SCIF accreditation. If approved, the owner of these devices and his/her supervisor must sign a statement acknowledging that they understand and will adhere to the restrictions identified below.
- Connection of a Personal PED to any IS within a SCIF is prohibited.
- PEDs with wireless, Radio Frequency (RF), Infrared (IR) technology, microphones, or recording capability will not be used unless these capabilities are turned off or physically disabled.

15.4.1.2. (U) Government Owned PEDs

- Government PEDs, hardware/software associated with them, and media must be controlled when entering/exiting a SCIF.
- Government PEDs are prohibited from operating within a SCIF unless authorized and accredited by the agency granting the SCIF accreditation. As part of the accreditation requirements, the user of these devices and his/her supervisor must sign a statement acknowledging that they understand and will adhere to the restrictions identified below.
- Connection of a Government PED to any IS within a SCIF must be approved by the ISSM in writing.
- PEDs with wireless, Radio Frequency (RF), Infrared (IR) technology, microphones, or recording capability will not be used unless these capabilities are turned off or physically disabled.
- Specified PEDs (i.e. Laptop Computers) may be used to process classified information. In addition, these PEDs may be granted approval to connect to ISs on a case-by-case basis in writing by the ISSM. Specified PEDs approved to process classified information must meet minimum technical security requirements.
- If approved, the PED and associated media must be transported and stored in a manner that affords security sufficient to preclude compromise of information, sabotage, theft, or tampering. Procedures for handling the PED in a SCIF must be available and provided to the user.

15.4.1.3. (U) Contractor Business Owned PEDs.

- Contractor Business Owned PEDs will follow all requirements identified in paragraph 15.4.1.2.
- All Contractor Business Owned PEDs must support a specific Government contract. Documented identification of the equipment in support of the contract must be provided prior to entry into a SCIF.

15.4.2. (U) Handling Procedures. When it has been determined that the use of PEDs is absolutely necessary to fulfill mission requirements, and the requirements set forth in paragraph 15.4.1 are satisfied, the following procedures must be implemented and followed.

15.4.2.1. (U) Standard Operating Procedure (SOP) Development. The responsible organization must develop a case specific SOP and/or ensure procedures are addressed in the site Concept of Operations (CONOP). The following information must be considered and, where applicable, included in the SOP:

15.4.2.1.1. (U) The SOP must include the organization and name of the Information Systems Security Manager (ISSM) and Special Security Officer (SSO) responsible for the issue and control of PEDs.

15.4.2.1.2. (U) Prior to the introduction of PEDs into a SCIF, it must be approved by the appropriate security personnel having security cognizance for the facility.

15.4.2.1.3. (U) PEDs must operate within one common accredited security parameter (i.e., protection level/level of concern, classification, etc.) as approved by the DAA Rep/SCO.

15.4.2.1.4. (U) All programs, equipment or data diskettes used with the PED must be marked with a label identifying the appropriate classification. Labeling exemption for operational security (OPSEC) requirements may be granted within local policy with DAA/DAA Rep/SCO concurrence.

15.4.2.1.5. (U) If unauthorized classified information is identified on a PED, procedures for control of the information and the PED must be established. For example, classified information on an unclassified PED may result in confiscation of the device as an incident (see Chapter 8).

15.4.2.1.6. (U) Every effort should be made to ensure that security control features are implemented when possible (e.g., access control through userid/password).

15.4.2.2. (U) SOP Approval. The organization requesting the use of PEDs must submit the SOP to the ISSM/SSO for coordination and approval.

CHAPTER 16

SECURITY PROCEDURES FOR INFORMATION SYSTEMS (IS) AND FACSIMILE (FAX) USE OF THE PUBLIC TELEPHONE NETWORK

16.1. (U) PURPOSE. This chapter outlines the minimum security requirements for the control and accounting of information systems (IS) and facsimile (FAX) use of the public telephone network. The Information System Security Manager (ISSM) is responsible for enforcing policy for the level of control and accounting appropriate for facsimile machine(s) within his/her site. This policy should be coordinated with the Service Certifying Organization (SCO) and the appropriate Special Security Officer (SSO). The potential for covert or inadvertent release of sensitive-but-unclassified (SBU) and classified information to an unintended destination is considered to be highly probable and is reduced significantly through rigorously enforcing policies and continuously monitoring these policies.

16.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

16.3. (U) PROCEDURES. External connectivity through the use of telephones or networks requires that users take every security precaution possible to prevent the loss of National Security Information (NSI) and SBU information via the public communications systems. **Classified information shall not be transmitted, processed or stored on any unclassified facsimile or an unclassified IS with either a modem or direct digital connection.** Telephone communications, voice or digital, must meet certain installation and equipment standards to ensure security. Telephone communications to external locations using computer-telephone connections must be approved before installation and activation to minimize the threat to the information.

16.3.1. (U) Facsimile (FAX) Connectivity:

16.3.1.1. (U) FAX Approval. The SSO, in coordination with the ISSM, is the approval authority for any facsimile operated within a SCIF. Specific FAX approval authority is delegated to command/site ISSMs who may approve unclassified and secure FAX machines within a SCIF. This authority is for single mode use only. ISSMs must ensure that any/all dual mode features are disabled. Dual mode (unclassified/secure) configurations are not approved for use in any facility under DIA/NSA cognizance. Transmission of information at levels above SI/TK (i.e., accountable SCI) requires applicable program manager's concurrence. Multi-function FAX/print machines with workstation/network connectivity/permanent storage/scan and text recognition capabilities are not to be approved for use of any feature other than secure facsimile transmission. Site ISSMs exercising SCI IS approval authority for these machines must ensure the following minimum security requirements are satisfied for unclassified and classified FAX connections. For non-inspectable space sites, coordinate with the organization TEMPEST officer and telephone control officer before installing any facsimile equipment in a secure area and for requests for telephone service in accordance with Telephone Security Guidelines (TSG).

16.3.1.1.1. **(U) Unclassified FAX.**

- Unclassified FAX machines must be clearly marked for unclassified use only and consent to monitoring notification.
- Any change of equipment or location must be locally documented, to include building/room, manufacturer/model, serial number, verification of SSO authorization and point of contact information.
- Multi-function FAX/print machines with workstation/network connectivity/permanent storage/scan and text recognition capabilities can not be approved, for unclassified use, by site ISSMs. Requests for this type of equipment should still be submitted via the DAA Rep/SCO.
- Sites should refer to local counsel on information that can be revealed in an unclassified FAX header.

16.3.1.1.2. **(U) Classified FAX**. Classified FAX is normally a connection of the output of a FAX to the input port of a STU-III/STE, whose encrypted output is connected to the unclassified telephone lines. The procedures defined in this chapter are in addition to the policy and procedures addressed in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 3013 or other appropriate SCI regulations. ISSMs are delegated approval authority for secure FAX machines operating up to the TS/SCI SI/TK level.

- Secure FAX machines must be clearly marked for the highest level of classified information processed.
- ISSMs will ensure that all operators understand the requirement to verify the level at which their STU-III/STE is connected to the recipient's STU-III/STE and verify the level at which the recipient is cleared before transmission commences.
- Information or additional compartments above the SI/TK level cannot be processed without prior approval from the appropriate data owner.
- The STU-III/STE is designed to prevent disclosure of information while it is being transmitted. Authorized users must verify the identity and clearance level of the distant party. If there is a human interface at the remote end, a challenge and reply authentication scheme will be used.
- The ISSM should approve only certified digital FAXes. The ISSM can obtain a list of certified secure digital facsimiles from the DAA/DAA Rep/SCO.

16.3.1.1.3. **(U) Non-Standard Secure FAXes.** A non-standard secure FAX consists of a group 3 (GS3) rated standard business FAX with an approved secure protocol adapter (SPA) and an approved STU-III/STE secure data terminal (SDT). In an effort to support cost effective alternatives to the certified list of digital FAXes, non-standard secure FAXes may be purchased and used with approval from the appropriate DAA. Memory in standard business FAX machines is not designed to meet any of the stringent requirements outlined above, and therefore cannot be trusted beyond the level of TS SI/TK when connected to an approved SPA (see www.nmic.ic.gov/security/products/secfax.html on INTELINK).

16.3.1.1.4. **(U) Procedures.** Each facsimile requires written standard operating procedures (SOP), or identified procedures within the site concept of operations (CONOP) that outline the security requirements for that system. The SOP shall be approved by the ISSM and include, at minimum, the following:

- Appropriate hardware marking requirements. For example, the unclassified facsimile must be clearly marked for the transmission of unclassified information only and must have consent to monitor stickers.
- Segregation from classified systems and media.
- Point of Contact authorized to monitor operations.
- A FAX cover sheet or equivalent will accompany each FAX transmission. This cover sheet will contain:
  - The number of pages transmitted;
  - The signature of the official approving the FAX transmission;

- The classification level of the overall information being transmitted;
- The sender's name and telephone number; and
- The intended recipient's name and telephone number.

- Audit logs will be used to record the transmission of any data over a FAX connected to a STU-III/STE. These logs will be maintained for one year and must include the following information:
  - User ID;
  - Date and time of FAX transmission;
  - The classification level of the information; and
  - The recipient's name, organization and telephone number.
- The ISSM will require the following minimum information to make an appropriate evaluation:
  - Building/Room Number FAX is located;
  - FAX manufacture/model number;
  - FAX Serial number;
  - Verification that the SSO has authorized the introduction of the equipment; and
  - Point of Contact's name and phone number.
- The following information should be documented and maintained with SCIF records:
  - location and/or location changes;
  - justification;
  - standard operating procedures;
  - identification of equipment (manufacturer, model, serial number, etc);
  - verification of SSO authorization;
  - approval level (matches the STU-III key); and
  - point of contact information.

16.3.1.1.5. **(U) FAX Accreditation.** All facsimile machines within a SCIF must be accredited by the site ISSM, or be previously accredited by the DAA Rep/SCO. All documentation and approval letters must be maintained with SCIF records.

16.3.2. (U) Computer-FAX/Modem Connectivity. A computer-FAX/modem provides a means for a computer to communicate data via telephone modem along a wired path to a distant end.

16.3.2.1. (U) Unclassified Computer-FAX/Modem Accreditation Approval. An SSAA/SSP, fully documenting the computer equipment to be used, shall be submitted to the ISSM. The SSAA/SSP will be processed via the SSO and ISSM for approval.

16.3.2.2. (U) Physical Disconnect of Unclassified Computer-FAX/Modems. The use of acoustic coupled modems is prohibited. Therefore, the physical disconnect of unclassified computer-FAX/modem equipment from the phone lines is not required.

16.3.3. (U) Computer-Modem Connectivity.

16.3.3.1. (U) Unclassified Computer-Modem Connectivity. Access to Commercial Internet Service Provider (ISP). "Dial-out" computer or data terminal access can only be to those unclassified systems deemed mission essential and approved in writing by the DAA Rep/SCO. Connectivity of unclassified systems to unclassified networks that are outside of SCIFs can pose a significant security risk.

16.3.3.1.1. **(U) ISP Connectivity.** The following procedures and guidelines pertain to those systems connected to networks which make it possible to connect to, or communicate with, any non-DoD IS.

16.3.3.1.1.1. (U) The system should be configured to present an unfavorable environment to any attacker, whether internal or external. The system should have only the functionality required for mission accomplishment. All other unnecessary services should be eliminated.

16.3.3.1.1.2. (U) The IS should use available auditing techniques to the fullest extent possible, to ensure the system is not compromised by attacks. Attacks may occur from across the network or from a legitimate system user. The System Administrator (SA) shall monitor audit logs regularly (preferably daily) and investigate any abnormalities which may indicate a security compromise. Any attacks detected against Government systems will be classified Confidential (at a minimum) and reported in accordance with Chapter 8.

16.3.3.1.1.3. (U) SA's should monitor all available resources that provide warnings of system vulnerabilities or on-going network attacks. Examples include advisories from the military service Computer Emergency Response Teams (CERT) (i.e., Air Force (AF) AFCERT, Navy NAVCIRT [Computer Incident Response Team], Army ACERT), and Automated Systems Security Incident Support Team (ASSIST) bulletins from the Defense Information Systems Agency (DISA).

16.3.3.1.2. **(U) IS to IS Connectivity.** The following procedures and guidelines deal with those systems connected only to independent IS systems, either point-to-point or within a community of interest (COI).

16.3.3.1.2.1. (U) The system should be configured to present an unfavorable environment to any attacker, whether internal or external. The system should have only the functionality required for mission accomplishment, eliminating unnecessary services.

16.3.3.1.2.2. (U) The IS should use available auditing techniques to the fullest extent possible, to ensure the system is not compromised by attacks. Attacks may occur from a legitimate system user. The System Administrator (SA) shall monitor audit logs regularly (preferably daily) and investigate any abnormalities which may indicate a security compromise. Any attacks detected against Government systems will be classified Confidential (at a minimum) and reported in accordance with Chapter 8.

16.3.3.1.2.3. (U) SA's should monitor all available resources that provide warnings of system vulnerabilities or ongoing attacks from connected IS. Examples include advisories from the military service Computer Emergency Response Teams (CERT) (i.e., Air Force (AF) AFCERT, Navy NAVCIRT [Computer Incident Response Team], Army ACERT), and Automated Systems Security Incident Support Team (ASSIST) bulletins from the Defense Information Systems Agency (DISA).

16.3.3.2. (U) Classified Computer-Modem Connectivity. The only mechanism for using a modem with classified communications is by first using NSA certified encryption mechanisms. Approval for such connections must be obtained from the DAA Rep/SCO.

16.3.3.3. (U) Classified Computer-STU-III/STE Data Port Connectivity. The following procedures and guidelines are established for using the data port of a STU-III/STE terminal and apply to all STU-III/STE users.

16.3.3.3.1. **(U) STU-III Data Port Connectivity within a SCIF.** Requests for STU-III/STE data port connections will be submitted to, and evaluated by the DAA Rep/SCO, on a case-by-case basis. An SSAA/SSP shall be submitted to the appropriate DAA Rep/SCO in accordance with Chapters 3 and 4 as applicable.

16.3.3.3.2 **(U) Identification and Authentication.** The STU-III/STE is designed to prevent disclosure of information while it is being transmitted. Authorized users must verify the identity and clearance level of the distant party. Access to a host IS must not be made using auto-answer capabilities unless the host IS enforces access controls for the connection separate from the communications link controls.

16.3.3.3.3. **(U) Connectivity Requirements.**
- For all connections of an IS or network to a STU-III/STE, the STU-III Security Access Control system (SACS) must be employed. Exceptions may be granted by the DAA Rep/SCO.
- The associated STU-IIIs/STEs must be keyed to the appropriate level to protect the data contained in the ISs.
- Community of Interest. All connected ISs using the STU-III/STE data port in a COI must be identified and accredited with identical Accredited Security Parameters (ASP) (classification levels, compartments, caveats, and mode of operation).

16.3.3.3.4. **(U) Connectivity Restrictions.** For all connections of an IS to a STU-III/STE data port, the following restrictions apply:
- Use of the STU-III/STE in the non-secure data mode is prohibited.
- Use of the STU-III/STE data port feature will be limited to connectivity of a specific set of STU-III/STE terminal units and ISs called a COI.
- The cable connecting an IS to a STU-III/STE data port must be installed in accordance with the National TEMPEST technical requirements.

CHAPTER 17

INTERCONNECTING INFORMATION SYSTEMS

17.1. (U) PURPOSE. This chapter describes policies, issues, and guidance for manual as well as automated processes that can be used to process and move sanitized and collateral information across these boundaries. The primary emphasis in managing information to support the war-fighter is to push information out of the SCI-controlled security domains into collateral security domains.

17.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	NO

17.3. (U) DISCUSSION. Policy requires that SCI information be safeguarded during all phases of operation, processing or storage on Information Systems (IS). This is required for individual ISs as well as ISs that are connected, particularly when operating at different levels. Different levels refers to two security domains which differ in some component of classification level, including respective compartments, sub-compartments, caveats, control markings or special handling marking. Different levels can also refer to the users (their security clearances, accesses, or need-to-know) of each respective system and the related Levels of Concern (LOC), Protection Level (PL), and the respective technical features implemented within each IS and security domain. When at least one system processes SCI, inter-domain connections will follow the TOP SECRET And Below Interoperability (TSABI) accreditation process.

17.3.1. (U) Interconnected Information Systems. Interconnected IS are composed of separately accredited ISs. Whenever separately accredited IS are interconnected, each DAA shall review the security attributes of each system to determine additional security requirements to be imposed. Such a determination will be based on: the technical operating level of each system (LOC/PL); the classification level of the information on each system; or the combination of users who have access to the respective IS. Respective DAAs shall document the interconnection requirements as part of the accreditation for the interconnected systems. Such interconnection determination also applies to support architecture connections, e.g., between networks.

17.3.2. (U) Inter-Domain Connections. When two different ISs are connected and the IS operate at different levels, the connection is an inter-domain connection. Any inter-domain connection, whether between IS or between networks, will comply with DCID 6/3, Section 7.B, Controlled Interface requirements, to provide appropriate confidentiality and integrity adjudication. The accreditation shall follow the TSABI process.

17.3.3. (U) Controlled Interface. The controlled interface requirements may be met by the IS devices themselves, or by a separate device or system added between two domains. Any IS or specific device (or combination) which facilitates the connection between two security domains, IS or networks, is considered a controlled interface. The specific requirements imposed on a controlled interface are highly dependent upon the expected flow of information between the two domains. All controlled interfaces have common requirements to maintain the integrity of the critical processes that control the information flow across the connections. These mandate physical protection of the controlled interface, preventing users from modifying the capabilities of the controlled interface, monitoring usage, and monitoring the interface for failure or compromise. In general, any protocols or services, which are not explicitly authorized, should be denied.

17.3.3.1. (U) One-Way Connections. When information flows in only one direction, the controlled interface requirements may be simplified, but are no less important. A controlled interface used in connection with controlling information flow in only one direction will shut off services and data flow in the reverse direction. The controlled interface may provide automated formatted or pre-determined acknowledge/non-

acknowledge messages which do not contain any substantive information to the source IS, without altering the designation as a one-way controlled interface.

17.3.3.1.1. **(U) Equal Classification Connections.** Connections between ISs or networks of equal classification occur when security domain levels are the same, but are maintained separate for other reasons, e.g. system technical features implemented on the respective IS or the set of users (their security clearances, accesses, or need-to-know).

17.3.3.1.2. **(U) Low-to-High Connections.** The information being passed from the low side will not have a confidentiality requirement; but the controlled interface will have to maintain the confidentiality of information at the high side from any exposure to the systems or users on the low side. The primary concern of a low-to-high connection is allowing information to flow without significant impairment but with appropriate integrity controls to protect the high side IS and their data. As more unstructured data types are identified for transfer, it becomes more difficult to prevent malicious code from being passed along with the desired information.

17.3.3.1.3. **(U) High-to-Low Connections.** The primary requirement for high-to-low connections is to protect the confidentiality of information that is not authorized for transfer to the low side. All information being transferred out of a domain, which has classified information which should not be passed across the boundary, will require a process that makes the determination on releasability. The processes that make this determination are called reliable review processes. These processes may be manual (reliable human review), automated (for highly formatted, integrity-wrapped, or reliably labeled information), or a combination depending upon the type and format of the data.

17.3.3.1.4. **(U) Other Unequal Classification Level Connections.** Sometimes, there is no real high/low relation between two domains, but simply a difference in information where separate data owners on each side of a connection have their own unique requirements. In this instance, each side is responsible for establishing the confidentiality controls and restrictions for review and release of information to the other side.

17.3.3.2. (U) Dual-Direction Connections. When information is expected to flow in both directions, the requirements of both low-to-high, high-to-low, and other equal or unequal level connections must be combined within the implementation of the controlled interface.

17.3.3.3. (U) Multi-Domain Connections. Some controlled interface devices are designed to provide support for connections between more than two domains simultaneously. The implementation for these connections should comply with the requirements for all of the individual combinations of paired connections within the controlled interface device (e.g., three domains have three connection pairs, four domains have six connection pairs, etc.).

17.3.4. (U) Review Procedures. Review procedures for all data transfers are discussed in further detail in 18.3.1.

17.3.4.1. (U) Reliable Human Review. Human review of information has to meet two aspects to be sufficient. First, a review of the information content to validate that it meets criteria for transfer across the domain boundary. Second, a technical review of the information as assembled to ensure that information normally hidden within a presentation is also authorized for transfer across the domain boundary. Any human review process conducted with an IS implements a combination of system capabilities to allow the human to conduct a review of the information. Presentation applications will help the human review data in its presentation form (e.g., a picture looks like a picture). Sometimes these applications will also meet the criteria for technical review by showing data in alternate forms including appended information. If these applications do not have this capability, then other applications may be required to complete technical data reviews. Because a human is interacting with automated processes to conduct reviews, the information being reviewed should have an integrity feature that validates that the review process does not alter the information being reviewed. This added capability is what makes the human review a reliable human review. Integrity and accountability requirements on the reliable human review process will require strong control of the information through the review process and control and accountability for the users associated with the reliable human review.

17.3.4.2. (U) Automated Review. When information is highly formatted, integrity-wrapped, or reliably labeled information, some automated processing may aid a human or may even make the decisions instead of a human. For automation to eliminate the reliable human review, the automated processes need to emulate all activities which would be performed by a human. When the information is not highly formatted, human review will still be required.

CHAPTER 18

INFORMATION TRANSFER AND ACCOUNTING PROCEDURES

18.1. (U) PURPOSE. This chapter outlines procedures for the transfer of information or software among Information Systems (ISs) of different classification levels using information storage media. The procedures are intended to protect the confidentiality of information on the media as well as other data on the end-point IS at different levels, prevent transfers of malicious code (Chapter 10 is germane), and prevent violation of legal copyright or license rights.

18.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

18.3. (U) PROCEDURES. This chapter outlines procedures for the transfer of classified information at varying levels to Information Systems (ISs) of different classification levels. For any system that operates with PL-3 and below functionality, media which is placed into that system must be classified at the highest level of information on the system until reviewed and validated. The following address proper classification determination during the access and transfer process.

18.3.1. (U) Reliable Human Review of Data. Human review is a process of validating the classification of data (classification level, compartments, sub-compartments, caveats, control markings or special handling marking) when it is stored or moved from an IS. Human review may be required for validating data classification for hardcopy prints (from systems with less than PL-4 labeling functionality), data being transferred to media, or manual transfers between security domains.

18.3.1.1. (U) Human review of information has to meet two criteria to be sufficient: a review of the information content to validate the actual classification level of the data, and a review of embedded or hidden information that is part of the data.

18.3.1.2. (U) Human review requires an individual who is knowledgeable of the subject matter to inspect the contents and provide validation of the data classification. This individual has to be able to see the information in its presentation form to make this determination.

18.3.1.3. (U) Information in its presentation form does not always show embedded or hidden data. This data may require a different process or application (or tools) to reveal the hidden data for the human review.

18.3.1.3.1. (U) Many users do not realize that DOS computers often store data on media in fixed length blocks, segments, or tracks. Because data records do not always fill the available space, residual information from memory is appended to the data record. The content of this information is unpredictable and may contain classified or other information from unrelated processes.

18.3.1.3.2. (U) Residual data that exists within information stored in memory gets copied as part of the data whenever it is duplicated.

18.3.1.4. (U) There are tools that can aid the human as he conducts the review process. Automated tools (e.g., BUSTER) can aid in the review of large amounts of data. A review of data is more reliable if it includes both a human review and review using automated tools. Reviews should not rely solely on an automated review unless the automated review process is approved by the appropriate DAA.

18.3.1.5. (U) Because a human is interacting with automated processes to conduct reviews, the information being reviewed should have an integrity feature so that the review process does not alter the information being reviewed. For example, write protect media before the information review.

18.3.1.6. (U) Reliable Human Review is the combination of the data content review, review for hidden data, and integrity controls applied to the information.

18.3.1.7. (U) A reliable human review may be a required component of a GUARD or Controlled Interface. Integrity and accountability requirements on the reliable human review process will require strong control of the information and its integrity through the review process, and added controls for accountability for the users associated with the reliable human review.

18.3.2. (U) Media Transfers In/Out of an Organization. All personnel will process outgoing media or report the receipt of media through the ISSM/ISSO or his/her designee before shipment out or use of such media. To ensure the correct classification (including unclassified) and appropriate labeling is being used, conduct reliable human review of 100% of information on the media. During the reliable human reviews, media should be write-protected so that no changes can occur. Identification of incorrect write protection requires installation of correct write protection and then proper conduct (or repetition) of the reliable human review. Virus policy prohibits movement of floppy disks between systems unless appropriate scanning procedures are implemented. If any problems are found, the media is not to be transferred or used, and appropriate reports will be generated and provided to the ISSM/ISSO. If the media is to be subsequently accounted for, make appropriate entries in the organization media accounting system.

18.3.3. (U) Disposition of Excess or Obsolete COTS Software. Software may be reused or released for resale only if:

- The software is still in its original unopened shipping wrapper.
- The user has personal knowledge that the software is not classified and is documented accordingly.

If the user cannot substantiate that the software is not classified, then he/she must ensure classified reutilization within the agency or organization or destruction by approved methods, as appropriate. Do not return the software to the issuing authority if it cannot be reused.

18.3.4. (U) High-to-Low Data Transfer by Media. This section addresses use of media to transfer information from a higher classified system to a lower classified system or a system with a different Accredited Security Parameters (ASP), including Unclassified. The procedures will differ based on the system capabilities present for different PL levels.

18.3.4.1. (U) PL-3 and Below Functionality. A local SOP must be written to outline the steps to protect the information when transferring data. The following general steps will be identified in the procedures and followed accordingly:

- The DAA Rep/SCO and ISSPM/ISSM must approve the procedures and individuals involved.
- Each transfer must be approved on a case-by-case basis by the ISSM/ISSO or designee.
- The media to be used in the process must be new.
- The information to be transferred is placed on the media. Then the media should be write-protected.
- Perform a reliable human review of 100% of the information as stored on the media to verify its classification level.
- Perform scanning of the media for viruses.
- Remove, validate write-protection and mark the media at the appropriate classification level as determined by the human review.
- The media may now be handled as marked.

18.3.4.2. (U) PL-4 and Above Functionality. A local SOP must be written to outline the steps to protect the information when transferring data. The following general steps will be identified in the procedures and followed accordingly:

- The DAA Rep/SCO and ISSPM/ISSM must approve the procedures and individuals involved.
- The media to be used in the process must be new.
- Copy the information to the media.
- Perform scanning of the media for viruses.
- Remove, write protect, and mark the media at the appropriate classification level (trusted from the PL-4 and above system).
- The media may now be handled as marked.

18.3.5. (U) Low-to-High Data Transfer by Media. This section addresses use of media to transfer information from a lower classified system, including unclassified, to a higher classified system or a system with a different ASP. A local SOP must be written to outline the steps to protect the media and systems involved when transferring data. One obvious reason for these procedures is to permit unclassified software such as Lotus and dBase to be installed into an IS containing classified information without requiring the media to become classified.

- The DAA Rep/SCO and ISSPM/ISSM must approve the procedures and individuals involved.
- The media to be used in the process must be new or an approved transfer disk that has been virus checked.
- Transfer information onto the media.
- Perform scanning of the media for viruses.
- When possible, ensure the transfer media is adequately write-protected if it is to remain classified at the lower level.
  - If the write-protect mechanism on the media is securely maintained, the media may remain at its lower classification level (the factory-write protect mechanism on a diskette is adequate).
  - If the write protect mechanism is not correctly maintained, the media must be marked and handled at the highest classification level with the most restrictive handling caveats of the information processed by the IS.
- Before transferring information to the higher classified system, perform scanning of the media for viruses.
- Transfer the data from the media to the higher classified IS.
- Following transfer, examine the write-protect device to validate that it is still securely intact.

Note: If the write protect is not maintained, then reclassify the media at the level of the target system.

18.3.6. (U) Demonstration Software. Floppy diskettes and removable hard disks used for demonstrations, with the intent of being returned to a vendor, must be processed on a computer that has never processed or stored classified data. Otherwise, the demonstration media cannot be released back to the vendor and should be destroyed. If returned to the vendor, a fully cleared and indoctrinated individual must verify that the media was used only in an unclassified computer.

CHAPTER 19

MULTI-POSITION SWITCHES

19.1 (U) PURPOSE. The purpose of this chapter is to provide the policy and procedures outlining the minimum requirements for the management of multi-position switches. This policy applies to all elements that use multi-position switches to share a common keyboard, mouse and monitor between different CPU's. These CPU's may process, store, produce, or transmit information of different classifications, compartments, sub-compartments, code words or releasability.

19.2. (U) SCOPE. This chapter states the policy for Key Board/Video/Mouse (KVM) or Key Board/Monitor/Mouse (KMM) Switches used to connect systems operating at different classification levels, compartments, sub-compartments, caveats, control markings or special handling marking under the cognizant security authority of DIA/NSA including those of contractors. This policy does not restrict the use of these types of devices based on the sensitivity of the information or levels of classification of the data processed on the CPU's that are shared. This policy applies to all individuals who have authorized access to these devices on the systems they use. Not all users are approved for this type of access, and this policy does not provide that approval or countermand in any way any restrictions already placed on the user for the use of these devices.

These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

19.3. (U) POLICY. Only KVM switches on the DIA Standard Products List for SCIFs accredited by DIA and KVM switches on the NSA Network Enterprise Solutions (NES) approved products list for SCIFs accredited by NSA shall be used within corresponding SCIFs when sharing a Key Board, Video Monitor or Mouse between CPUs at different classification levels. KVM switches currently in use that do not meet tempest or AIS requirements must be replaced with DIA/NSA approved switches by 31 December 2001. Authorizations are required from the DAAs of the respective systems when using a KVM switch to share the Key Board, Video Monitor, or Mouse. The DAAs are DIA for JWICS, NSA for NSANET, and the Defense Information Systems Agency (DISA) for NIPRnet and SIPRnet. The use of switchboxes for print services between classification levels is prohibited. Switchboxes may be used between the same classification levels for print services.

19.4. (U) RESPONSIBILITIES.

19.4.1. (U) DAA Rep.
- Ensure all authorizations from DAAs of respective systems are obtained.

19.4.2. (U) ISSM.
- Maintain the KVM Switch User Agreements files.
- The ISSM will verify that the user has the necessary training and complies with the requirements for the introduction and use of multi-position switches.

19.4.3. (U) ISSO/System Administrator.
- Ensure that the systems are approved by the configuration Management Board.
- Ensure that the systems are installed correctly and meet all TEMPEST Standards.
- Ensure the desktop banners, backgrounds, and screen locks have the proper classification banner.

19.4.4. (U) User.
- Protect the Information System and KVM in your area.
- Report any spillage of classified information in accordance with the JDCSISSS.
- Safeguard and report any unexpected or unrecognized computer output, including both displayed or printed products in accordance with JDCSISSS.
- Use different passwords on each system connected through a KVM.
- Ensure that the classification level is displayed by each systems screen lock and that the password is required to regain entry to the system.
- Ensure that the systems screen lock is invoked if the system is left unattended of if there is a 15-minute period of inactivity for each system.
- Responsible for marking/maintaining magnetic media IAW Chapter 13 of JDCSISSS.

19.5. (U) AIS REQUIREMENTS. The introduction and use of multi-position switches in a SCI environment presents a moderate degree of risk to classified or sensitive information and systems. Therefore, all users will be responsible for the management of these devices. To minimize the risk of inadvertently entering information onto the wrong network, the following requirements must be met.

19.5.1. (U) Labels. All information systems components must be labeled in accordance with DCID 6/3, Paragraph 8.B.2 (a and b). All switch positions, cables, and connectors must be clearly marked with the appropriate classification labels.

19.5.2. (U) Desktop Backgrounds. To avoid inadvertent compromises, systems joined by multi-position switches will utilize desktop backgrounds that display classification banners at the top or bottom. The classification banner will state the overall classification of the system in large bold type, and the banner background will be in a solid color that matches the classification (SCI - yellow, Top Secret - orange, Secret - red, Confidential - blue, Unclassified - green). When systems have a similar classification level, but require separation for releasability or other constraints, use of unique colors for the different systems is permissible.

19.5.3. (U) Screen Locks. Screen Lock applications must display the maximum classification of the system on which the system is currently logged into and shall implement a lockout feature to re-authenticate the user.

19.5.4. (U) Smart Keys/Permanent Storage Medium. Systems using KVM switches must not employ “smart” or memory enhanced/data retaining keyboards, monitors or mice. These types of interfaces provide memory retention that creates a risk of data transfer between systems of different classifications.

19.5.5. (U) Hot Key Capability. Switches that support "Hot-Key" capability to switch, toggle or otherwise affect the switching between CPUs are prohibited.

19.5.6. (U) Scanning Capability. Switches with the ability to automatically scan and switch to different CPUs are prohibited.

19.5.7. (U) Wireless or Infrared Technology. Systems using KVM switches must not use keyboards or mice with wireless or infrared technology

19.5.8. (U) Unique Password Requirement. At a minimum, users must ensure that they use different/unique passwords for each system connected through a multi-position switch. Whenever possible, system administrators should employ different logon USERIDs to help users further distinguish between the systems.

19.5.9. (U) Data Hierarchy. Data of a higher classification must not be introduced to a system of a lower classification.

19.5.10. (U) Security CONOPS. A site with a requirement for multi-position switches must include the KVM procedures within the site's Security Concept of Operations (SECONOPS). The approval authority will be the Site ISSM.

19.5.11. (U) Training. ISSMs/ISSOs/Supervisors will ensure user training and compliance to the requirements associated with the introduction and use of multi-position switches.

19.5.12. (U) TEMPEST. Blanket approval to install keyboard, video, mouse (KVM) switches is granted within DIA accredited Sensitive Compartmented Information Facilities (SCIFs) located within the US and meeting NSTISSAM TEMPEST/2-95A, 3 Feb 00, recommendation “I” (having 100 meters of inspectable space) as defined by the SCIF's TEMPEST accreditation document from DIA/DAC-2A. Blanket approval to install keyboard, video, mouse (KVM) switches is granted within NSA accredited Sensitive Compartmented Information Facilities (SCIFs) located within the US and meeting NSTISSAM TEMPEST/2-95A, 3 Feb 00, Zones C and D having more than 100 meters of inspectable space. Prior approval is required for overseas facilities and all other recommendations.

19.5.13. (U) Procedures for LOGON/Switching Between Systems.

Logging on to systems.
- Identify the classification of the system currently selected.
- Use the login and password appropriate to that system.
- Verify the classification of the present system by checking the classification label.
- Begin processing.

Switching between systems.
- Select desired system with the multi-position switch.
- Verify the classification of the present system by checking the classification label.
- Begin processing at the new classification level.

EXCEPTIONS. Any exception to this policy requires approval of the DAA Rep responsible for the Certification/accreditation of systems in your SCIF.

19.6. (U) KVM SWITCH USER AGREEMENT. The user agreement (Figure 19-1) documents training and certification for personnel using the KVM switch.

KVM USER AGREEMENT FORM

1. (U) KVM SWITCH USER AGREEMENT. The user agreement documents training and certification for personnel using the KVM switch.

1.1. (U) Procedures for LOGIN and Switching Between Systems. This process must be performed for each switch between systems. When the DoDIIS system is not selected, it is required to be screenlocked.

1.1.1. (U) Logging Onto a System.

- Identify the classification of the system currently selected
- Use the login and password(s) appropriate to that system
- Verify the classification of the present system by checking the classification label
- Begin Processing

1.1.2. (U) Switching Between Systems.

- For DoDIIS systems, screenlock the system you are currently working on. For NSA systems, ensure that each system's screenlock is invoked if there is a 15 minute period of inactivity.
- Select desired system with the KVM switch.
- Enter your user id and password to deactivate the screen lock.
- Verify the classification of the present system by checking the classification label.

1.1.3. (U) Logging Off of a System.

- Close all applications processing on the active system
- Logout of the system when processing in no longer required on the system
- Logout of system at the end of duty day

1.2. (U) A weekly inspection of tamper seals (if any) will be performed by the user.

1.3. (U) Any suspected tampering and/or mishandling of KVM will be reported to your site ISSM.

_____

Printed Name of User

_____

Signature _____ Date _____

The above individual has received the necessary training and has complied with the requirements for application and use of KVM switches

_____

Printed Name of ISSM

_____

Signature _____ Date _____

FIGURE 19.1 (U) KVM SWITCH USER AGREEMENT FORM.

CHAPTER 20

CLEARING, SANITIZING, AND RELEASING COMPUTER COMPONENTS

20.1. (U) PURPOSE. The purpose of this chapter is to provide guidance and procedures to clear and sanitize magnetic storage media that is no longer useable, requires transfer, or should be released from control. These procedures apply to all Information Systems (IS) containing electronic, electromagnetic, electrostatic, or magnetic storage media. For clarification, Magnetic storage media is considered to be any component of a system which, by design, is capable of retaining information without power.

20.2. (U) SCOPE. These procedures are effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

20.3. (U) RESPONSIBILITIES. The Information Systems Security Manager (ISSM) is responsible for the security of all ISs and media assigned to the organization and under his/her purview. To protect these assets, he/she must ensure the security measures and policies contained within this chapter are followed. Additionally, the ISSM will publish supplemental organizational procedures (Standard Operating Procedures [SOPs], etc.), if needed, to implement the requirements herein.

20.4. (U) PROCEDURES. The procedures contained below meet the minimum security requirements for the clearing, sanitizing, releasing, and disposal of magnetic media as well as guidance for other types of information storage media. These procedures will be followed when it becomes necessary to release magnetic media, regardless of classification, from Sensitive Compartmented Information (SCI) channels. Media that has ever contained SCI, other intelligence information, or Restricted Data can not be sanitized by overwriting; such media must be degaussed before release.

20.4.1. (U) Review of Terms. To better understand the procedures contained herein, it should be understood that overwriting, clearing, purging, degaussing, and sanitizing are not synonymous with declassification. The following are definitions:

20.4.1.1. (U) Clearing. Clearing is the process of removing information from a system or the media to facilitate continued use and to preclude the AIS system from recovering previously stored data. In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval. Clearing can be accomplished by overwriting or degaussing.

20.4.1.2. (U) Sanitizing (Also Purging). Sanitizing is the process of removing information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. In general, laboratory techniques cannot retrieve data that has been sanitized/purged. Sanitizing may be accomplished by degaussing.

20.4.1.3. (U) Destruction. Destruction is the process of physically damaging media so that it is not usable and there is no known method of retrieving the data.

20.4.1.4. (U) Declassification. Declassification is an administrative process used to determine whether media no longer requires protection as classified information. The procedures for declassifying media require Designated Approving Authority (DAA) Representative (Rep) or Service Certifying Organization (SCO) approval.

20.4.1.5. (U) Periods Processing. Provided the sanitization procedures between each protection level segment have been approved by the DAA Rep/SCO based on guidelines from the data owner(s) or responsible official(s), the system need meet only the security requirements of each processing period, while in that period. If the sanitization procedures for use between periods are approved by the DAA Rep/SCO, the security requirements for a given period are considered in isolation, without consideration of other processing periods. Such sanitization procedures shall be detailed in the SSAA/SSP.

20.4.2. (U) Overwriting Media. Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing. However, the effectiveness of the overwrite procedure may be reduced by several factors: ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps. Software overwrite routines may be corrupted by hostile computer viruses. Overwriting is not an acceptable method to declassify media.

20.4.2.1. (U) Overwriting Procedure. The preferred method to clear magnetic disks is to overwrite all locations with a pseudo-random pattern twice and then overwrite all locations with a known pattern.

20.4.2.2. (U) Overwrite Verification. The overwrite procedure must be verified by the ISSM or his/her designee.

20.4.3. (U) Degaussing Media. Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

20.4.3.1. (U) Magnetic Media Coercivity. Magnetic media is divided into four types (I, II, IIA, III) based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercivity must be ascertained prior to executing any degaussing procedure.

20.4.3.2. (U) Types of Degausser. The individual performing the physical degaussing of a component must ensure that the capability of the degausser meets or exceeds the coercivity factor of the media, and that the proper type of degausser is used for the material being degaussed. The four types of degaussers are:

- Type I. Used to degauss Type I media (i.e., media whose coercivity is no greater than 350 Oersteds [Oe]).
- Type II. Used to degauss Type II media (i.e., media whose coercivity is no greater than 750 Oe).
- Type IIA. Used to degauss Type IIA media (i.e., media whose coercivity ranges from 751 to 900 Oe).
- Type III. Used to degauss Type III media (i.e. media whose coercivity ranges from 901 to 1700 Oe). Currently, there are no degaussers that can effectively degauss all Type III media. Some degaussers are rated above 901Oe, and their specific approved rating will be determined prior to use.

20.4.3.3. (U) Degausser Requirements. Refer to the current issue of the National Security Agency (NSA) Information Systems Security Products and Services Catalogue (Degausser Products List Section), for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to assure continued compliance with the appropriate specification. National specifications provide a test procedure to verify continued compliance with the specification.

20.4.3.4. (U) Use of a Degausser. Once a degausser has been purchased and has become operational, the gaining organization must establish a SOP explaining how it will be used. The degausser must be certified annually.

20.4.4. (U) Sanitizing Media. Tables 20-1 and 20-2 provide instructions for sanitizing data storage media and system components.

TABLE 20.1. (U) SANITIZING DATA STORAGE MEDIA

MEDIA TYPE	PROCEDURE(S)

Magnetic Tape	
Type I	a or b
Type II,IIA	b
Type III	Destroy
Magnetic Disk Packs	
Type I	a or b
Type II,IIA	b
Type III	Destroy
MEDIA TYPE	**PROCEDURE(S)**
Magnetic Disks	
Floppies	a or b, then Destroy
Bernoullis	Destroy
Removable Hard Disks	a or b
Non-Removable Hard Disks	a or b
Optical Disks	
Read Only (including CD-ROMs)	Destroy
Write Once, Read Many (WORM)	Destroy
Read Many, Write Many	Destroy
PROCEDURES	
These procedures will be performed or supervised by the ISSO.	
a. Degauss with a Type I degausser. See 20.4.3.2.	
b. Degauss with a Type II, IIA degausser. See 20.4.3.2.	

TABLE 20.2. (U) SANITIZING SYSTEM COMPONENTS

TYPE OF COMPONENT	**PROCEDURE(S)**
Magnetic Bubble Memory	a or b or c
Magnetic Core Memory	a or b or d
Magnetic Plated Wire	d or e
Magnetic-Resistive Memory	Destroy
SOLID STATE MEMORY COMPONENTS	
Dynamic Random Access Memory (DRAM) (Volatile)	e and i
if RAM is functioning	d, then e and i
if RAM is defective	f, then e and i
Static Random Access Memory (SRAM)	j
Programmable ROM (PROM)	Destroy (see h)
Erasable Programmable ROM (EPROM/UVPROM)	g, then c and i
Electronically Erasable PROM (EEPROM)	d, then i
Flash EPROM (FEPROM)	d, then i
PROCEDURES	
These procedures will be performed or supervised by the ISSO.	
a. Degauss with a Type I degausser.	
b. Degauss with a Type II,IIA degausser.	
c. Overwrite all locations with any random character.	
d. Overwrite all locations with a random character, a specified character, then its complement.	
e. Remove all power, including batteries and capacitor power supplies from RAM circuit board.	
f. Perform three power on/off cycles (60 seconds on, 60 seconds off each cycle, at a minimum).	
g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.	
h. Destruction required only if ROM contained a classified algorithm or classified data.	
i. Check with the ISSPM/DAA Rep/SCO to see if additional procedures are required.	
j. Store a random unclassified test pattern for a time period comparable to the normal usage cycle.	

20.4.5. (U) Destroying Media. Data storage media will be destroyed in accordance with DAA/DAA Rep/SCO approved methods.

20.4.5.1. (U) Expendable Item Destruction. Expendable items (e.g., floppy diskettes and hard drives) are not authorized for release and reuse outside of the SCI community after they have been degaussed (Table 20.1). If these items are damaged or no longer deemed usable, they will be destroyed. When destroying, remove the media (magnetic mylar, film, ribbons, etc.) from any outside container (reels, casings, hard cases or soft cases, envelopes, etc.) and dispose of the outside container in a regular trash receptacle. Cut the media into pieces (a crosscut chipper/shredder may be used to cut the media into pieces) and then burn all pieces in a secure burn facility or pulverize to 25mm (3/16-inch) specification. If the Environmental Protection Agency (EPA) does not permit burning of a particular magnetic recording item, it will be degaussed, cut into pieces (a chipper/shredder preferred) and disposed of in a regular trash receptacle.

Note: Use of a burn bag does not necessarily mean that organizations actually burn. Many organizations have pulverization facilities that handle all burn bags.

20.4.5.1.1. (U) Below are the shipping instructions for destruction of other classified items to include floppy discs, typewriter ribbons, magnetic tapes that have been removed from the reels, film, viewgraphs, chips, circuit boards and paper. Paperwork required is either an SF153 Destruction Form or a DD1149 (shipping document). POC is at NSA LL14, commercial (301) 688-5467/DSN 644-5467 (NSTS 972-2486);

COMSEC MATERIAL, send by regular mail to:
DIRNSA ATTN: LL14
Account #889999
Fort Meade, MD 20755-6000

NON-COMSEC MATERIAL CLASSIFIED UP TO AND INCLUDING SECRET, send by regular mail to:
National Security Agency
ATTN: CMC - LL14 - Suite 6890
9800 Savage Road
Fort George G. Meade, MD 20755-6000

NON-COMSEC MATERIAL CLASSIFIED HIGHER THAN SECRET, send by DCS to:
449563 - BA20
Film Destruction Facility

20.4.5.2. (U) Destruction of Hard Disks and Disk Packs:

20.4.5.2.1. **(U) Hard Disks.** Hard disks are expendable items and are not authorized for release and reuse outside of the SCI community. Each item is considered classified to the highest level of data stored or processed on the IS in which it was used. If hard disks are damaged, or no longer deemed usable, they will be degaussed and then destroyed. If the platter(s) of the defective unit can be removed and the removal is cost effective, then destruction of a hard disk consists of dismantling the exterior case and removing the platter from the case then degaussing the platter. Techniques which remove the recording surface (grinding or chemical etching the oxide surface) prior to disposal do not enhance security and are unnecessary. They may be disposed of by using approved procedures for the destruction or disposal of unclassified metal waste.

20.4.5.2.2. **(U) Shipping Instructions.** Below are the shipping instructions for destruction of magnetic media, including cassette tapes, videotapes, hard discs, optical disks (including CDs) and magnetic tapes on reels. Paperwork required is either a DD1149 (shipping document) or 1295A (transmittal of classified material document). POC is at NSA LL14, (301) 688-7631 DSN 644-7631 (NSTS 977-7249).

CLASSIFIED UP TO AND INCLUDING SECRET, send by regular mail to:
National Security Agency
9800 Savage Road
Fort George Meade, MD 20755-6000

SAB-3, Suite 6875
Attn: LL14, Degaussing

CLASSIFIED HIGHER THAN SECRET, send via Defense Courier Service (DCS) to:
449276-BA21
DIRNSA, FT MEADE
Degaussing

CLASSIFIED EQUIPMENT UP TO AND INCLUDING SECRET, send by regular mail :

National Security Agency
9800 Savage Road
Fort George Meade, MD 20755-6000

SAB-4, Suite 6629
Attn: S713 Cleansweep

CLASSIFIED EQUIPMENT HIGHER THAN SECRET, send via Defense Courier Service (DCS) to:

449276-BA21
DIRNSA, FT MEADE
CLEANSWEEP

20.4.5.2.3. **(U) Disk Packs.** Each item is considered classified to the highest level of data stored or processed on the IS in which it was used. If disk packs are damaged, or no longer deemed usable, they will be degaussed and then destroyed. Techniques which remove the recording surface (grinding or chemical etching the oxide surface) prior to disposal do not enhance security and are unnecessary. They may be disposed of by using approved procedures for the degauss and destruction or disposal of unclassified metal waste.

20.4.5.2.4. **(U) Optical Storage Media.** Optical mass storage, including compact disks (CD, CDE, CDR, CDROM), optical disks (DVD), and magneto-optical disks (MO) shall be declassified by means of destruction. Optical media shall be destroyed by burning, pulverizing, or grinding the information bearing surfaces. When material is pulverized or ground, all residue must be reduced to pieces sized 0.25mm (3/16-inch) or smaller. Burning shall be performed in an approved facility certified for the destruction of classified materials; residue must be reduced to white ash.

20.4.6. (U) Malfunctioning Media. Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing will be reported to the Information System Security Officer (ISSO)/System Administrator (SA). The ISSO/SA will coordinate the repair or destruction of the media with the ISSM and responsible DAA Rep/SCO. If the hard drive is under a warranty which requires return of the hard drive, dismantle the hard drive and return the case but do not send the platter to the manufacturer.

20.4.7. (U) Release of Memory Components and Boards. Prior to the release of any malfunctioning components proper coordination, documentation, and written approval must be obtained. This section applies only to components identified by the vendor or other technically-knowledgeable individual as having the capability of retaining user-addressable data; it does not apply to other items (e.g., cabinets, covers, electrical components not associated with data), which may be released without reservation. For the purposes of this chapter, a memory component is considered to be the Lowest Replaceable Unit (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release (See Table 20-2). Memory components are specifically handled as either volatile or nonvolatile, as described below.

20.4.7.1. (U) Volatile Memory Components. Memory components that **do not** retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system, are considered volatile memory components. Volatile components that have contained extremely sensitive or classified information may be released only in accordance with procedures developed by the ISSM, or designee, and documented in the SSAA/SSP. A record must be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remains in or on the component when power is removed.

20.4.7.2. (U) Nonvolatile Memory Components. Components that **do** retain data when all power sources are discontinued are nonvolatile memory components. Some nonvolatile memory components (e.g., Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM)) and their variants that have been programmed at the vendor's commercial manufacturing facility, and are considered to be unalterable in the field, may be released. All other nonvolatile components (e.g., removable/non-removable hard disks) may be released after successful completion of the procedures outlined in Table 20-2. Failure to accomplish these procedures will require the ISSM, or designee, to coordinate with the DAA Rep/SCO to determine releasability.

20.4.7.3. (U) Other Nonvolatile Media: Media that do retain data when all power sources are discontinued are nonvolatile media and include:

20.4.7.3.1. **(U) Visual Displays.** A visual display may be considered sanitized if no sensitive information is etched into the visual display phosphor. The ISSO should inspect the face of the visual display without power applied. If sensitive information is visible, destroy the visual display before releasing it from control. If nothing is visible, the ISSO/SA shall apply power to the visual display; then vary the intensity from low to high. If sensitive information is visible on any part of the visual display face, the visual display shall be destroyed before it is released from control.

20.4.7.3.2. **(U) Printer Platens and Ribbons.** Printer platens and ribbons shall be removed from all printers before the equipment is released. One-time ribbons and inked ribbons shall be destroyed as sensitive material. The rubber surface of platens shall be sanitized by wiping the surface with alcohol.

20.4.7.3.3. **(U) Laser Printer Drums, Belts, and Cartridges.** Laser printer components containing light-sensitive elements (e.g., drums, belts, complete cartridges) shall be sanitized before release from control.

20.4.7.3.3.1. (U) Elements containing intelligence information shall be sanitized in accordance with the policy contained in the Director of Central Intelligence Directive (DCID) 1/21.

20.4.7.3.3.2. (U) Used toner cartridges from properly operating equipment that properly completed the last printing cycle may be treated, handled, stored and disposed of as UNCLASSIFIED.

20.4.7.3.3.3. (U) When a laser printer does not complete a printing cycle (e.g., a paper jam or power failure occurs) completing a subsequent print cycle before removal of the cartridge is sufficient to wipe residual toner from the cartridge drum.

20.4.7.3.3.4. (U) If the toner cartridge is removed without completing a print cycle, inspect the cartridge drum by lifting the protective flap and viewing the exposed portion of the drum. If residual toner is present, manually rotating the drum is sufficient action to wipe off residual toner material present.

20.4.7.3.3.5. (U) After completing actions for incomplete print cycles, the toner cartridge may be treated, handled, stored and disposed of as UNCLASSIFIED.

20.4.8. (U) Clearing Systems for Periods Processing. Systems authorized for periods processing must be cleared of any information which is not authorized between the different defined periods of mode/level of operation. All system components must be cleared in accordance with guidance of this chapter.

20.4.8.1. (U) Most systems will have volatile memory components. These components can be cleared by removing power (turning the system off).

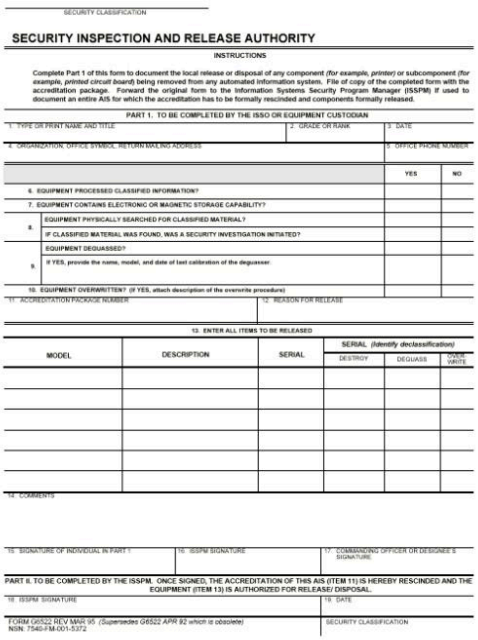
20.4.8.2. (U) Some systems have removable media designed to save time and be more convenient for changing between modes/levels (e.g., this avoids having to overwrite the media and re-install all of the software including complex operating system software). The IS should be shut down before the removable media is exchanged.

20.4.8.3. (U) Nonvolatile memory components which are significant components of a system could retain information between the periods. When relying on removable media, the system should have no significant nonvolatile memory components which could contain unauthorized information remaining within the system.

- Any system approved for periods processing will be prohibited from containing nonvolatile memory or a fixed hard drive.
- For example, a PL-2 system with a removable hard drive "for data" which is interchanged between periods is not sufficient if a permanent hard drive remains inside the IS with "just the operating system". The PL-2 system does not provide sufficient controls to trust against unauthorized information inadvertently being stored to the operating system hard drive.

20.4.9. (U) Release of Systems and Components. The ISSM, or designee, shall develop equipment removal procedures for systems and components and these procedures shall be stated in the SSAA/SSP. When such equipment is no longer needed, it can be released if:

- It is inspected by the ISSM, or designee. This inspection will assure that all media, including internal disks, have been removed or sanitized.
- A record is created of the equipment release indicating the procedure used for sanitization and to whom the equipment was released. The record of release shall be retained for a period prescribed by the DAA Rep/SCO.
- Procedures specified by the DAA Rep/SCO are used.



SECURITY CLASSIFICATION

SECURITY INSPECTION AND RELEASE AUTHORITY

INSTRUCTIONS

Complete Part 1 of this form to document the local release or disposal of any component *(for example, printer)* or subcomponent *(for example, printed circuit board)* being removed from any automated information system. File of copy of the completed form with the accreditation package. Forward the original form to the Information Systems Security Program Manager (ISSPM) if used to document an entire AIS for which the accreditation has to be formally rescinded and components formally released.

PART 1. TO BE COMPLETED BY THE ISSO OR EQUIPMENT CUSTODIAN

1. TYPE OR PRINT NAME AND TITLE | 2. GRADE OR RANK | 3. DATE

4. ORGANIZATION, OFFICE SYMBOL, RETURN MAILING ADDRESS | 5. OFFICE PHONE NUMBER

	YES	NO
6. EQUIPMENT PROCESSED CLASSIFIED INFORMATION?		
7. EQUIPMENT CONTAINS ELECTRONIC OR MAGNETIC STORAGE CAPABILITY?		
8. EQUIPMENT PHYSICALLY SEARCHED FOR CLASSIFIED MATERIAL?		
IF CLASSIFIED MATERIAL WAS FOUND, WAS A SECURITY INVESTIGATION INITIATED?		
9. EQUIPMENT DEGAUSSED?		
If YES, provide the name, model, and date of last calibration of the degausser.		
10. EQUIPMENT OVERWRITTEN? (If YES, attach description of the overwrite procedure)		

11. ACCREDITATION PACKAGE NUMBER | 12. REASON FOR RELEASE

13. ENTER ALL ITEMS TO BE RELEASED

MODEL	DESCRIPTION	SERIAL	SERIAL (Identify declassification) DESTROY	DEGAUSS	OVER-WRITE

14. COMMENTS

15. SIGNATURE OF INDIVIDUAL IN PART 1 | 16. ISSPM SIGNATURE | 17. COMMANDING OFFICER OR DESIGNEE'S SIGNATURE

PART II. TO BE COMPLETED BY THE ISSPM. ONCE SIGNED, THE ACCREDITATION OF THIS AIS (ITEM 11) IS HEREBY RESCINDED AND THE EQUIPMENT (ITEM 13) IS AUTHORIZED FOR RELEASE/ DISPOSAL.

18. ISSPM SIGNATURE | 19. DATE

FORM G6522 REV MAR 95 *(Supersedes G6522 APR 92 which is obsolete)* NSN: 7540-FM-001-5372 | SECURITY CLASSIFICATION

20.4.9.1. (U) Documenting IS Release or Disposal. The National Security Agency/Central Security Service (NSA/CSS) Form G6522, shown in Figure 20.1, or similar form/documentation, will be used to document the local release or disposal of any IS or processing component.

FIGURE 20.1. (U) SAMPLE NSA/CSS FORM G6522

CHAPTER 21

OTHER SECURITY REQUIREMENTS

21.1. (U) PURPOSE. The purpose of this chapter is to provide information on subject matter which does not require a specific chapter to cover the areas addressed.

21.2. (U) SCOPE. These procedures could be effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	YES
DESIGN PHASE	YES
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

21.3. (U) REQUIREMENTS:

21.3.1. (U) Contingency Planning. A contingency plan is a plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program. It consists of a comprehensive statement of all the actions to be taken before, during, and after a disaster or emergency condition along with documented and tested procedures. It ensures that critical resources are available and facilitates the continuity of operations in an emergency situation.

21.3.1.1. (U) Backup. Preventing catastrophic loss of data and progress requires that users maintain adequate backups for their stored data. Besides preventing data loss, backups of data for archiving purposes allow for proper on-line storage management. All magnetic media must be properly labeled and protected according to Chapter 13.

21.3.1.2. (U) Responsibilities. Each Information Systems Security Manager (ISSM), or designee, will develop locally needed backup plans. The plans should consider data-production rates and data-loss risks when under development. The areas of risk that should be identified and planned for are:

21.3.1.2.1. **(U) Immediate Losses.** Ensures that the risk of a power failure and the resulting loss of data is worked at the time of power loss. Develop policy and procedures which reflect these risks. For example, if one were creating a word-processing document when power loss occurred, the document would be lost if the user had not made periodic "saves" while creating it. Some word-processing systems allow the user to make periodic saves automatically (for example, Word for Windows). Most applications do not have this capability, and the users must be made aware of this potential problem.

21.3.1.2.2. **(U) Media Losses.** Develop a local procedure which reflects this risk. If a hard disk were dropped or contaminated in some way, the disk backups, coupled with periodic incremental backups between full backups, would allow you to restore the data close to the condition it was in before the loss. Keep "active backups" for disks which contain often-used applications.

21.3.1.2.3. **(U) Archiving Inactive Data.** Develop procedures to manage the disk space. For example, old correspondence might be put onto a disk for archiving purposes. Thus, you could create a list of all files and file descriptions which could be returned to the active users.

21.3.2. (U) Foreign National Access to Systems Processing Classified Information:

21.3.2.1. (U) U.S. Government classified information is not releasable to foreign nationals except as authorized by the U.S. Government.

21.3.2.2. (U) Data owners can designate their information as releasable to individuals of specific nationalities. The Principle Accrediting Authority (PAA)/Designated Approving Authorities (DAA) shall obtain the written permission of all applicable data owners before allowing access by foreign nationals to a system that contains information that is not releasable to individuals of those nationalities.

21.3.2.3. (U) The decision to allow foreign nationals access to systems that process classified information shall be explicit and shall be in writing. This includes controls over foreign national access or proximity to systems that process NOFORN classified information.

21.3.2.4. (U) If a proposed IS serves as a controlled interface connection to an IS with foreign national users, the IS must meet controlled interface requirements of DCID 6/3 Section 7. The DAA Rep/SCO must ensure that written concurrence for the controlled interface is obtained from data owners and affected DAAs prior to permitting implementation of the connection. Controlled interfaces which connect to an IS that processes SCI information must be accredited through the TOP SECRET And Below Interoperability (TSABI) process as noted in Chapter 17.

21.3.2.5. (U) Foreign national ISs may only be allowed in shared SCIF facilities with formal joint approval. Connections between IS are only permitted among systems at the same classification level, upon the approval of the PAA.

21.3.3. (U) Tactical/Deployable Systems. There are more aspects to tactical or deployed systems than increased threat from their mobile status. These systems not only have "additional" security requirements, but also have to deal with the issue of tactical/operational requirements that may conflict with SCI security requirements. Tactical/operational requirements for near-continuous operation and high availability conflict with security requirements, specifically the automated information protection features that enforce access control and restriction features which can be expected within an office/base environment.

21.3.3.1. (U) Resolving Conflicting Requirements. When presented for DAA approval, the DAA may require alternate security requirements or safeguards for tactical systems while in transit or in the tactical environment. The DAA may approve the IS security requirements based on the system accreditation documentation of the specific operational requirements. The DAA should specifically list all such approval decisions in the accreditation documentation for the IS. Examples of tactical/deployable systems and their security implementations that require DAA attention are as follows.

21.3.3.1.1. (U) IS which process SCI information may be developed specifically for tactical environments, implemented with tactical/operational features that are contrary to SCI information security requirements.

21.3.3.1.2. (U) Tactical systems may be introduced into SCI environments for tactical processing at the SCI level, which could require modification to meet SCI information requirements.

21.3.3.1.3. (U) Generalized systems may be developed which are intended for use in both environments. These systems need a capability to alternate between meeting the respective requirements of each environment.

21.3.3.2. (U) Specific Conflicting Requirements. The following is a collection of security requirements that have direct conflict with tactical/operational requirements.

21.3.3.2.1. **(U) Audit Process Requirements.**

- Security requirement: If the Audit process fails, the system is unable to provide monitoring for unauthorized activities and should not continue operating, but should default to a safe/secure posture pending restoring the ability to maintain proper audit.

- Operational requirement: Failure of the Audit process should not interfere with continued normal operation of a system.
- Sample security implementation: Allow the system to continue operation if the Audit process fails.

21.3.3.2.2. **(U) Audit log requirements.**
- Security requirement: If the Audit logs fill up and the system is unable to record the monitoring information for unauthorized activities, it should not continue operating, but should default to a safe/secure posture pending proper retrieval/storage/archive of the audit data.
- Operational requirement: Full audit logs should not interfere with normal operation of a system. Audits may fill up due to other than normal activities required to support operations, or a system administrator being too busy responding to another operational requirement.
- Sample security implementation: Placing operational requirements ahead of security requirements could result in the Audit process being set for "overwrite oldest if full" or FIFO overwrite.

21.3.3.2.3. **(U) Protection for Information against unattended operation.**
- Security requirement: When a terminal is not attended, screen savers, screen locks, and deadman lockout features provide protection of classified information. These features can interrupt an operation when a terminal is left in a monitoring mode while other evolutions are taking place.
- Operational requirement: Long term monitoring may be required without continuous user interaction with a system. Rapid response may require eliminating delays resulting from required security passwords on screen locks. The need for rapid response could also completely obviate Deadman timeout features.
- Sample security implementation: disable these features for the IS for use in the tactical environments.

21.3.3.2.4. **(U) Labeling media and hardware components.**
- Security requirement: Removable media and IS hardware components should be labeled in accordance with Chapter 13.
- Operational requirement: Operational security (OPSEC) requirement to disguise the existence of classified information on an IS (including specification of compartments).
- Sample security implementation: Reusable, deployed hardware sanitized for travel (media removed) is shipped via commercial carrier to its intended destination, no labels present.

21.3.3.2.5. **(U) Use of group accounts.**
- Security requirement: Individual accountability for all users requires individual accounts which can be monitored through automated audit capabilities (see DCID 6/3).
- Operational requirement: Use of group user accounts in a tactical/watchstanding environment allows rapid interchange between users whose primary focus is quick access to the system without interruption of functions or capabilities. This also avoids system transients (and potential for errors on startup) as the system is shut down and restarted for a different user to logon.
- Sample security implementation: Lists do exist for watchstander rotations or battle station assignments, which could be retained and used to augment activity logs to correlate user identities to actions as recorded on audit logs. Advanced alternative: Developers provide a simple pop-up "change USERID" GUI which does not cause the system to shutdown or change operations, but which simply changes accountability via the new USERID/password for continuing processes for an individual member of a common functional group.

21.3.4. (U) Guest systems in a SCIF. SCIFs are accredited under the authority of either DIA or NSA. Any system that enters the SCIF which has not already been certified or accredited by the respective cognizant SCIF authority is considered a Guest system. These guest systems may be brought into the SCIF only at the discretion of the cognizant authority and the local SSO/ISSM/ISSO as long as prudent AIS Security measures and documentation are in place. An SSO is responsible for all resident SCI information, including that which exists on AIS within a SCIF. The ISSM/ISSO supports the SSO in all security matters related to AIS, and the DAA who accredits SCI systems within that SCIF is directly associated with the authority that established the SCIF, i.e., the cognizant DAA. Systems that process SCI under the cognizance of DIA and NSA have clear guidance as provided within this document. The following are three examples of guest systems:
- SCI or SAPI systems already certified by another PAA;
- SCI systems that have no existing certification; and
- Unclassified systems or systems with classification levels lower than SCI.

21.3.4.1. (U) SCI Systems With Certification. Within the DCID 6/3 community of PAAs, there is common acceptance of system accreditation and certification for systems that process SCI/SAPIs. These systems may be brought into a SCIF along with the certification documents provided by the PM/PMO so that the SCIF cognizant DAA may accredit the systems as they are connected to existing architectures. The ISSM will ensure that appropriate system documentation from the PM/PMO is available to the DAA/DAA Rep/SCO to support the accreditation prior to the system installation. If the guest systems will operate independently (not connecting to or through existing architectures), the SSO/ISSM may accept the systems with accreditation as delivered and document the presence of these systems on configuration management architectures.

21.3.4.2. (U) SCI Systems Without Certification. For SCI systems that do not have existing certification, the PM/PMO will provide appropriate documents for SCI Security certification and accreditation in accordance with Chapters 3 or 4.

21.3.4.3. (U) Unclassified or Collateral Systems. Non-SCI systems that are to be operated within a SCIF also require a certification/accreditation. These systems may be certified/accredited by an appropriate authority other than the cognizant SCI DAA. When the local Commander/SSO authorizes such systems to enter the SCIF and operate, then a coordinated policy/agreement should be established that addresses the security and operational interests of the different DAAs. The PM/PMO will deliver accreditation documentation for the systems to the SSO/ISSM with the request to install.

21.3.4.3.1. (U) When a decision is made to allow GENSER or unclassified systems into a SCIF, a policy/agreement must be developed and documented by the SSO/ISSM. The SSO and ISSM are responsible for implementing appropriate security operating procedures before the respective systems/networks are permitted to enter the SCIF. These procedures will need to address IS security issues not already documented.

21.3.4.3.2. (U) Recommended issues to be included within the local procedures:
- Define the extent that the SSO/ISSM will have purview over the other DAA's systems while they are operated within the SCIF. This is an item that can be addressed in an MOA.
- Define the authority responsible for the respective systems and the SSO who retains oversight responsibility for SCI information within the SCIF.
- Document the coordination between SSO/ISSM in establishing the SCI controls for systems within a SCIF.
- ___Document TEMPEST countermeasures (e.g., update Fixed Facility Checklist and RED/BLACK separation compliance with Inspectable Space Determination).
- ___Develop an SOP for managing systems/media that are allowed to enter/depart the facility on a regular or recurring basis.

21.3.5. (U) Other Requirements. DCID 6/3 provides specific requirements for additional system functions that are not covered in other sections of this document.
- Dedicated Servers.
- Embedded and Special Purpose IS.
- Web Security - Clients.
- Servers
- E-Mail
- Collaborative Computing.
- Distributed Processing.

CHAPTER 22

INFORMATION SYSTEMS (IS) AND NETWORK SECURITY SELF-INSPECTION AID

22.1. (U) PURPOSE. The purpose of this chapter is to provide an aid for the inspection, certification, and accreditation of Sensitive Compartmented Information (SCI) ISs. The checklist is based upon the criteria contained in this document and other applicable Department of Defense (DoD) security regulations/directives. This checklist can be used as follows:
- To inspect IS operations periodically throughout their life cycle
- To inspect organizational IS security program
- Incorporated as part of an organization's self-inspection program
- In preparation for formal inspections, IS certifications and accreditations

22.2. (U) SCOPE. This aid is effective in the following life cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	NO
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

22.3. (U) APPLICABILITY. This checklist is applicable to those systems and security programs that support DoD SCI operations. The ISSM/ISSO should periodically complete the checklist (recommended annually).

22.4. (U) PROCEDURES. The completion of this self-inspection checklist is basically self-explanatory and may be locally reproduced to meet the self-inspection and IS certification and accreditation requirements of an organization.

Table 22.1 (U) IS AND NETWORK SECURITY SELF-INSPECTION CHECKLIST

IS AND NETWORK SECURITY SELF-INSPECTION CHECKLIST			
SECTION A - IS SECURITY PROGRAM MANAGEMENT	**YES**	**NO**	**NA**
1. Has an IS and Network Security Program been established?			
2. Has the responsible authority appointed an ISSM in writing?			
3. Have ISSOs been appointed in writing and does the ISSM maintain a copy of the appointment letter?			
4. Has the ISSM appointment letter been forwarded to the Designated Approving Authority (DAA) /DAA Representative (REP)/Service Certifying Organization (SCO), and is a copy on file at the unit?			
5. Are signs posted throughout the organization with the names and phone numbers of the Security Officers?			
6. Is the IS Security Program being supported by supervisors and senior managers?			
7. Has the ISSM and ISSOs completed an appropriate training course (ND 225, Operational Information System Security Course, or the Department of Defense Intelligence Information Systems (DoDIIS) Site ISSM Course or equivalent course)?			
8. Has an IS Security Training Program been established to ensure DoD certification of SAs, ISS personnel and IS users?			

9. Has a self-inspection of the organization IS and Network Security Program been conducted?			
10. Have identified deficiencies been documented?			
11. Does the responsible authority review self-inspection reports to ensure follow-up actions are taken ~~on~~ to correct all identified deficiencies?			
12. Have all identified deficiencies been corrected?			
13. Have all ISs been certified and accredited prior to operation or an IATO granted?			
14. Are appropriate IS security regulations/policy documents being maintained, and are they accessible to the ISSM, ISSO, SA and system users?			
15. Are the following on file and used effectively to manage the organization's IS & Network Security Program?			
a. HQs-level advisory messages.			
b. Policy letters and directives.			
c. SSAA/SSPs and any associated approval to operate documentation.			
d. SCIF Accreditation Documentation.			
e. Advisory messages from the Defense Information Systems Agency's (DISA) Automated System Security Incident Support Team (ASSIST) and the Service's Computer Emergency/Incident Response Team (CERT/CIRT).			
f. Risk analysis and vulnerability reports.			
g. TEMPEST checklists, certificates, and waivers, if applicable, for all installed ISs?			
h. Self-inspection reports and appropriate follow-up actions.			
16. Are assistance visits conducted to assist subordinate units (if any) in the development of their IS & Network Security Programs?			
17. Are all personnel aware of their responsibilities in reporting IS incidents and violation?			
18. Are the results of security incidents/violations investigated, reported IAW applicable regulations, and reviewed to determine whether changes to IS policy/procedures are required?			
19. Is a functional Configuration Management Program in place?			
SECTION B - ACCREDITATION AND CERTIFICATION			
20. Has an System Security Authorization Agreement [SSAA]/ Systems Security Plan [SSP]) been:			
a. Developed for the Information Systems?			
b. Properly coordinated within the organization (ISSM, ISSO/SA, Physical Security personnel, TEMPEST Officer, etc.)? {TEMPEST change icw Chapter 6?}			
c. Reviewed by the ISSM for appropriate action?			
d. A file copy maintained by ISSM/ISSO?			
e. Has the ISSM/ISSO coordinated the accreditation documentation with their CCB?			
f. Is appropriate accreditation/IATO documentation maintained by ISSM/ISSO for each IS?			
g. Forwarded to the appropriate DAA/DAA Rep/SCO?			
21. Is the SSAA/SSP updated as follows:			
a. When hardware/software configuration changes occur?			
b. When the system is relocated?			
c. When the security mode/protection level changes?			
d. When connected to additional networks?			
e. Upon the three year anniversary date?			
22. Have all external connections to installed ISs been validated and approved by the DAA Rep/SCO?			
23. Are the ISSM/ISSOs aware of the SABI/TSABI process when connecting systems/networks of different classifications?			
SECTION C - IS & NETWORK SECURITY			
24. Are systems which process SCI information located in areas according to DCID 1-21?			
25. Is only authorized software being used?			
26. Are the ISSM, ISSOs/SAs, and users knowledgeable of virus protection and reporting procedures?			
30. Is virus software current?			
31. Are all IAVA actions implemented, verified and documented?			
32. Are documented software patches current and installation dates documented?			
33. Are Audit Trails:			
a. Being implemented?			
b. Reviews being limited to the ISSM, or alternate, and ISSOs/SAs?			
c. Being reviewed at the required interval, and appropriate action taken, where applicable?			
d. Summary reports and SCI system audits being maintained for five years?			
34. Is the Access Request and Verification Roster:			
a. Acknowledged and signed?			
b. Periodically validated?			
c. Updated to indicate final access removal?			
d. Appropriately classified?			
e. Maintained by the SA?			
35. Are passwords changed quarterly for SBU and other classified systems, at least semiannually for SCI systems, or when other conditions (e.g. a change in job status, TDY over 60 days, compromise) occur?			
36. Are passwords protected at the same level as the information they protect?			
37. Do all user passwords contain a minimum of eight alphanumeric characters?			
38. Are the ISSOs/SAs implementing the appropriate countermeasures to protect against vulnerabilities?			
39. Are procedures in effect to ensure the proper classification markings of all computer-generated products?			
40. Are IS components (CPU, monitor, printer, scanner) marked with appropriate classification labels (e.g. 700-series or equivalent)?			
41. Is formal documentation used (i.e. 6522 or equivalent form) to record all IS release actions; are they completed and verified by appropriate IS personnel and filed with the SSAA/SSP?			
42. Are DD254s reviewed periodically to validate contractor access to data on SCI IS?			
43. Has an IS Contingency Plan:			
a. Been developed?			
b. Been successfully tested in the past year?			
c. Been periodically reviewed and updated?			
44. Does the approved SSAA/SSP and unit Standard Operating Procedures (SOPs) cover the following security related topics:			
a. Procedures for securely bringing the system up/down?			
b. Security responsibilities encompassing all personnel?			
c. Security marking of output products?			
d. Procedures for downgrading and/or releasing output or media?			
e. Procedures for media degaussing, destruction, and/or downgrading?			
f. Procedures for generating and reviewing the audit data?			
g. Procedures for adding/removing users from the IS/LAN?			
h. Procedures establishing access control privileges for users?			
i. Operational Security (OPSEC)?			
j. Virus and Incident reporting procedure?			
k. Contingency Plan procedures?			
l. Information Storage Media control and accounting procedures?			
m. Password Management procedures?			

n. Procedures for obtaining appropriate authorization to conduct monitoring of suspicious or illegal activity?			
45. Is the audit data protected by the Security Support Structure (operating system or security software)?			
46. Are the following audit reports generated to aid in the periodic review of auditable anomalous activity:			
a. Invalid logon attempts showing an abnormal number of aborted access attempts by the same user, or from the same terminal?			
b. Access to the system during non-duty hours?			
c. Attempts to use special privileges (e.g. SUPERUSER) for activities other than system restoration; for example, changing a users accesses or privileges?			
d. Movement of data to information storage media?			
e. Invalid file access attempts to include READ, WRITE, EXECUTE and DELETE?			
f. Invalid access attempts to Audit Trail data files?			
g. Override attempts of computer generated output classification markings?			
h. Attempts to print a file for which a user ID is not authorized?			
47. Have unique IS ID and Password controls been implemented on the IS/LAN?			
48. Are passwords suppressed when entered?			
49. Do three consecutive unsuccessful log-in attempts from a single access port or against a single user ID result in the terminal or user ID being disabled?			
50. Are data access controls automatically set to limit access when any new file or data set is created?			
51. Are system privileges limited to those necessary to perform assigned tasks (e.g. SUPERUSER, System Programmers, etc.)?			
52. Are the following features installed and activated?			
a. Screen Blanking			
b. Screen Lock			
c. Deadman Timeout			
53. Are appropriate Government warning banners and labels being used on systems?			
54. If an IS is connected to a STU-III/STE data port, has permission been received from the proper authority?			
55. Are unclassified ISs connected directly to the public telephone network; if so, has approval been received from proper authority?			
56. Are approved keyboard-monitor-mouse (KMM) switches installed between IS which are connected to a network or another IS at different classification levels?			
57. Are appropriate procedures implemented and followed in using KMM switches?			
58. Has the proper authority approved the use of the KMM?			
59. Is the use of dial-in modems connected to ISs/LANs IAW applicable policy?			
60. Has the proper authority approved the use of the dial-in modems?			
61. Is the Auto Answering feature of all STU-IIIs/STEs configured IAW applicable policy?			
62. Has the proper authority approved the use of the STU-III/STE Auto Answering feature?			
63. Are communications links connecting the components of the IS processing classified or sensitive unclassified information protected IAW National COMSEC policies?			
64. Are all critical systems backed up by an Un-interruptible Power Supply (UPS) system?			
65. Is the Red/Black separation criteria being strictly enforced?			
SECTION D - IS MAINTENANCE			
66. Has a maintenance policy and procedure been developed and implemented?			
67. Are maintenance personnel cleared?			
68. Are maintenance personnel U.S. citizens?			
69. Are uncleared maintenance personnel escorted by fully cleared and technically qualified personnel?			
70. Are IS components purged of all classified or unclassified information prior to removal from IS spaces, and are these actions appropriately documented?			
71. Are storage media removed from ISs prior to being released for service or repair?			
72. Are areas sanitized prior to maintenance performed by unclear personnel?			
73. Is a maintenance log, documenting repairs, used and maintained?			
74. Are controls in place for maintenance of diagnostic hardware or software?			
SECTION E - DECLASSIFICATION			
75. Are procedures in effect to ensure the calibration requirements for degaussers are being followed and they are operating effectively?			
76. Is the degausser recalibrated yearly?			
77. Are only approved degaussers utilized for the declassification of magnetic media?			
78. Is documentation on all IS media declassification actions being maintained?			
79. Are printer ribbons appropriately destroyed and handled at the same classification level as its associated IS?			
80. Are toner cartridges properly cleared before turn-in for reuse?			
81. Are controls in place for maintenance or diagnostic hardware or software?			
SECTION F - INFORMATION STORAGE MEDIA CONTROL			
82. Has a SOP been written outlining the procedures to be followed for the introduction and removal of storage media into and out of secure facilities IAW national policy?			
83. Has the Cdr/Commanding Officer publicized/developed policy identifying the level of control and accountability of information storage media in the organization?			
84. Have procedures been developed for the control of information storage media IAW national-level policy?			
85. Are media marked and labeled with the correct classification and handling instructions (Standard 700 series labels or equivalent, Privacy Act, Special Access Programs [SAP], etc.)?			
86. Does the ISSM ensure excess or obsolete commercial software is free of classified information prior to release or reuse?			
87. Are procedures established which outline steps to be taken when transferring data to and from systems of unequal accreditation (classification and/or sensitivity)?			
88. Are reused removable media used at the same or higher classification level?			

APPENDIX A

REFERENCES

(U) The following publications are the primary security regulations associated with, and affecting Information Systems (IS) Intelligence operations. This appendix is not an inclusive list of all security regulations.

PUBLIC LAWS

Computer Fraud and Abuse Act, 18 U.S. Code section 1030, 1984.
Electronic Communications Privacy Act, 18 U.S. Code Section 2510, 1986.
Public Law 100-235, The Computer Security Act of 1987, 8 January 1988.

EXECUTIVE ORDERS

Executive Order 12333, United States Intelligence Activities, 4 December 1981.
Executive Order 12829, National Industrial Security Program, 6 January 1993.
Executive Order 12958, Classified National Security Information, 20 April 1995.

NATIONAL PUBLICATIONS

Common Criteria for Information Technology Security Evaluation, CCIB-98-026, Version 2.0, May 1998.

DCID 6/3, Director of Central Intelligence (DCI) Directive (DCID) 6/3, Protecting Sensitive Compartmented Information within Information Systems, 6 June 1999.
DCID 1/19, Security Policy Manual for Sensitive Compartmented Information and Security Policy Manual, 1 March 1995.
DCID 1/21, Physical Security Standards for SCIFs, 29 July 1994.
DCID 2/12, Community Open Source Program, 1 March 1994.
The Intelligence Community Open Source Strategic Plan, 21 April 1993.
NSTISSAM TEMPEST/2-95, National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95 (formerly NACSIM 5203), Red/Black Installation Guidelines, 12 December 1995.
NSTISSI 3013, National Security Telecommunication and Information Systems Security Instruction (NSTISSI) 3013, Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type 1 Terminal, 8 February 1990.
NSTISSI 4009, National Security Telecommunication and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary, January 1999.
NSTISSI 7000, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7000, TEMPEST Countermeasures For Facilities, 29 November 1993.
NSTISSI 7003, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003 (C/NF), Protected Distribution Systems, 13 December 1996.
NSTISSP 300, National Security Telecommunications and Information Systems Security Policy (NSTISSP) 300, National Policy on Control of Compromising Emanations, 29 November 1993.
OMB Circular A-130, Management of Federal Information Resources, 15 July 1994, and principally, Appendix III, Security of Federal Automated Information, February 1996.

DEPARTMENT OF DEFENSE (DoD) PUBLICATIONS

DoD 5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual (U), August 1998.
DoD Directive 5200.1-R, Information Security Program Regulation, January 1997.
DoD Directive 5200.2-R, Policy on Investigation and Clearance of DoD Personnel for Access to Classified Defense Information, 15 February 1986
DoD Directive C-5200.5, Communications Security (COMSEC), 21 April 1990.
DoD Directive C-5200.19, Control of Compromising Emanations, 16 May 1995.
DoD Directive 5200.28, Security Requirements for Automated Information Systems (AIS), 21 March 1988.
DoD Directive 5215.1, Computer Security Evaluation Center, 25 October 1982.
DoD Directive 5220.22, DoD Industrial Security Program, 8 December 1980.
DoD 5220.22-R, Industrial Security Regulation, December 1985.
DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995, and its Supplement, dated February 1995.
DoD Directive 5240.4, Reporting of Counterintelligence and Criminal Violations, 22 September 1992.
DoD Trusted Computer System Evaluation Criteria (Orange Book of the Rainbow Series), December 1985.

DEFENSE INTELLIGENCE AGENCY (DIA) PUBLICATIONS

DIA Manual 50-4, Department of Defense (DoD) Intelligence Information Systems (DoDIIS) Information Systems Security (INFOSEC) Program, 30 April 1997.
DIA Regulation 50-2, Information Security Program, 15 July 93
Defense Intelligence Management Document SC-2610-141-93, DoDIIS Site Information Systems Security Officer's (ISSO) Handbook, November 1993.
Defense Intelligence Management Document DS-2610-142-00, DoD Intelligence Information System (DoDIIS) Security Certification and Accreditation Guide April 2000.
Defense Intelligence Management Document SC-2610-143-93, DoDIIS Site Certifier's Guide, November 1993.
The Intelligence Community Open Source Strategic Plan, 21 April 1993.

NATIONAL SECURITY AGENCY (NSA)/CENTRAL SECURITY SERVICE (CSS) PUBLICATIONS

NSA/CSS Circular 25-5, Systems Acquisition Management, 3 April 1991.
NSA/CSS Circular 90-11, Protected Wireline Distribution System for COMINT Facilities, 7 June 1993.
NSA/CSS Classification Guide 75-98, 20 February 1998.
NSA/CSS Directive 21-1, DoD Computer Security Center Operations, 29 March 1984.
NSA/CSS Directive 130-1, Operational Information System & Network Security Policy, 17 October 1990.
NSA/CSS Manual 130-1, Operational Computer Security, October 1990.
NSA/CSS Manual 130-2, Media Declassification and Destruction Manual, November 2000.
NSA/CSS Regulation 110-2, The NSA/CSS ADP Program, 27 November 1981.
NSA/CSS Regulation 120-1, Reporting of Security Incidents and Criminal Violations, 16 March 1989.
NSA/CSS Regulation 120-24, STU-III Security Requirements, 20 February 1990.
NSA/CSS Regulation 130-2, Computer Virus Prevention Policy, 13 January 1993.
NSA/CSS Regulation 130-3, Security Testing of NSA/CSS Automated Information Systems (AIS) and Networks, 24 July 1992.
NSA/CSS Regulation 130-4, Computer Security for Connection of an Automated Information System (AIS) to the STU-III (type 1) Terminal Data Port, 27 July 1993.
NSA/CSS Regulation 130-5, Use of Unclassified Publicly Accessible Computer Networks and information Systems such as the INTERNET (U), 15 July 1996.
USSID 12, United States Signals Intelligence (SIGINT) Directive 12, Automatic Data Processing (ADP) Policy for SIGINT Operations, 20 October 1980.
NSA/CSS Information Systems Certification and Accreditation Process (NISCAP), 15 October 2000

APPENDIX B

GLOSSARY OF ACRONYMS, ABBREVIATIONS, AND TERMS

ACRONYMS AND ABBREVIATIONS

(U) The following acronyms/abbreviations are expanded for clarification.

ACERT	Army Computer Emergency Response Team
AF	Air Force
AFCERT	Air Force Computer Emergency Response Team
AIA	Air Intelligence Agency
AIS	Automated Information System
ASP	Accredited Security Parameters
ASSIST	Automated Systems Security Incident Support Team
AUTODIN	Automatic Digital Network
BDS	Broadband Distribution System
C&A	Certification and Accreditation
CCB	Configuration Control Board
CD	Compact Disk
CDE	Compact Disk Extra
CD-R	Compact Disk-Read
CDR	Critical Design Review
CD-ROM	Compact Disk-Read Only Memory
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CM	Configuration Management
CMB	Configuration Management Board
CO	Commanding Officer
COI	Community Of Interest
COMINT	Communications Intelligence
COMNAVSECGRU	Commander Naval Security Group
COMSEC	Communications Security
CONOP	Concept of Operation
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CRYPTO	Cryptologic
CSE	Client-Server Environment
CSS	Central Security Service
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving/Accrediting Authority
DAA Rep	Designated Approving/Accrediting Authority Representative
DAC	Discretionary Access Control
DCI	Director, Central Intelligence
DCID	Director of Central Intelligence Directive
DEXA	DoDIIS Executive Agent
DIA	Defense Intelligence Agency
DIAM	Defense Intelligence Agency Manual
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DMS	Defense Messaging System
DoD	Department of Defense
DoDIIS	Department of Defense Intelligence Information Systems
DOS	Disk Operating System
DRAM	Dynamic Random Access Memory
DSN	Defense Switching Network
DVD	Digital Video Disk
EEFI	Essential Elements of Friendly Information
EEPROM	Electronically Erasable Programmable Read Only Memory
EO	Executive Order
EPA	Environmental Protection Agency
EPROM	Erasable Programmable Read Only Memory
ERB	Engineering Review Board
FAX	Facsimile
FEPROM	Flash Erasable Programmable Read Only Memory
FOUO	For Official Use Only
FTS	Federal Telecommunications Service
FW&A	Fraud Waste & Abuse
GENSER	General Service
GOTS	Government Off-The-Shelf
HOIS	Hostile Intelligence Services
HQ	Headquarters
HSO	Host Security Office
IA	Information Assurance
IATO	Interim Approval To Operate
IAVA	Information Assurance Vulnerability Assessment
IAW	In Accordance With
IA	Information Assurance
ID	Identification
IG	Inspector General
INSCOM	Intelligence and Security Command
IOC	Initial Operational Capability
IR	Infrared
IS	Information System
ISD	Inspectable Space Determination
ISS	Information System Security
ISSE	Information Systems Security Engineer
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSPM	Information Systems Security Program Manager
JAG	Judge Advocate General
LAN	Local Area Network
LOC	Level-of-Concern
LRU	Lowest Replaceable Unit
MILNET	Military Network
MO	Magneto-Optical
MOU	Memorandum Of Understanding
NACSIM	National COMSEC Information Memorandum
NAVCIRT	Navy Computer Incident Response Team
NCS	National Cryptologic School
NIMA	National Imagery and Mapping Agency
NIPRNET	uNclassified Internet Protocol Router NETwork
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NISSIB	NSA/CSS Information System Security Incident Board
NOFORN	No Foreign National
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSI	National Security Information
NSN	National Stock Number
NSO	Network Security Officer
NSTISSAM	National Security Telecommunications Information Systems Security Advisory Memorandum
NSTISSC	National Security Telecommunications Information System Security Committee
NSTISSI	National Security Telecommunications Information System Security Instruction
NSTISSP	National Security Telecommunications Information System Security Policy
Oe	Oersteds
OPSEC	Operational Security
PAA	Principal Accrediting Authority
PDA	Personal Digital Assistant
PDD	Personal Digital Diary

PDR	Preliminary Design Review
PDS	Protected Distribution System
PED	Portable Electronic Device
PL	Protection Level
PM	Program Manager
PMO	Program Management Office
POC	Point of Contact
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RF	Radio Frequency
RFI	Radio Frequency Interference
ROM	Read Only Memory
SA	System Administrator
SACS	Security Access Control System
SAP	Special Access Program
SAPI	Special Access Program - Intelligence
SBU	Sensitive But Unclassified
SCE	Service Cryptologic Element
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCO	Service Certifying Organization
SDD	Secure Data Device
SDSO	System Design Security Officer
SF	Standard Form
SI	Special Intelligence
SIGAD	SIGINT Address
SIGINT	Signals Intelligence
SIM	System Integration Management
SIMO	System Integration Management Office
SIO	Senior Intelligence Officer
SISSPM	Senior Information Systems Security Program Manager
SOP	Standard Operating Procedure
SOW	Statement Of Work
SRAM	Static Random Access Memory
SSAA	System Security Authorization Agreement
SSAN	Social Security Account Number
SSO	Special Security Office/Special Security Officer
SSP	System Security Plan
STE	Secure Telephone Equipment
STU-III	Secure Telephone Unit III
ST&E	Security Test and Evaluation
T&E	Test and Evaluation
TDY	Temporary Duty
TK	Talent Keyhole
TS	Top Secret
UCMJ	Uniform Code of Military Justice
UPS	Un-interruptible Power Supply
US	United States
USERID	User Identification
USSID	United States Signals Intelligence Directive
USSS	United States SIGINT System
WAN	Wide Area Network
WORM	Write Once Read Many

TERMS

The following terms and definitions have been extracted from various documents and are provided for information and clarification. They are restricted to issues addressing information systems and related security matters.

Access. The ability and means to communicate with (input to or receive output from), or otherwise make use of any information, resource, or component in an information system (IS); or to have authorized entry to a specified area.

Accreditation. The official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. This authorization is granted by the appropriate Designated Approving Authority (DAA), on a case-by-case basis, permitting the processing of SCI information on an IS. Approval is based upon the DAA's review of the SSAA/SSP. Under certain conditions interim approval-to-operate (IATO) may be granted by designees of the DAA.

Accredited Security Parameters (ASP). The security classification levels; compartments and subcompartments at which an information system (IS) or network is accredited to operate (e.g. Top Secret [TS]/Special Intelligence [SI]/Talent Keyhole [TK]).

Authentication. (1) To establish the validity of a claimed identity. (2) To provide protection against fraudulent transactions or logons by establishing the validity of a USERID, message, station, individual or originator.

Availability. Timely, reliable access to data and information services for authorized users.

BLACK. A designation applied to telecommunications and information systems (ISs), and to associated areas, circuits, components, and equipment, in which only unclassified signals are processed.

Broadband Distribution System (BDS). Any broadband system which can carry multiple channels of information. A BDS is not a local area network (LAN), however, it is capable of being the backbone for multiple LANs.

Buster. A computer program - part of the Computer Security Toolbox. BUSTER is a MS-DOS based program used to perform a binary search of a disk or diskette for any word or set of words found in a search definition file by performing a linear search on a disk or diskette, four sectors at a time. BUSTER uses the "LIMITS.TXT" file as its document for search word patterns.

Certification. The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a set of specified security requirements.

Certified TEMPEST Technical Authority (CTTA). A U.S. Government or U.S. Government contractor employee designated to review the TEMPEST countermeasures programs of a federal department or agency.

Classified Information. National security information (NSI) that has been classified pursuant to Executive Order 12958.

Clearing. Removal of data from an IS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

Collateral. (1) Classified Non-Sensitive Compartmented Information (SCI) material to include General Service (GENSER) - an intelligence community term. (2) All national security information (NSI) classified under the provisions of an Executive Order (EO) for which special Intelligence community systems of compartmentation (i.e., SCI) are not formally established.

Command Authority. The individual responsible for the appointment of user representatives for a department, agency, or organization and their key ordering privileges.

Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Community-of-Interest (COI). A restricted network of users, each having an information system (IS) with an accredited security parameter identical to the others and having the need to communicate securely with other members of the network.

Compromising Emanations. Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled or otherwise processed by telecommunications or information systems (IS) equipment. (See TEMPEST).

Computer Security (COMPUSEC). See INFOSEC.

Computer Security Toolbox. A set of tools designed specifically to assist Information Systems Security Officers (ISSOs)/System Administrators (SAs) in performing their duties. The functions within the TOOLBOX can erase appended data within files, eliminate appended data in free or unallocated space, search for specific words or sets of words for verifying classification and locating unapproved shareware programs. It also includes a program which allows you to clear laser toner cartridges and drums.

Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Control. The process of controlling modifications to a telecommunications or information system (IS) hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

Configuration Management. The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation of an information system (IS), throughout the development and operational life of the system.

Connectivity. A word which indicates the connection of two systems regardless of the method used in physical connection.

Contingency Plan. A plan maintained for emergency response, backup operations, and post-disaster recovery for an information system (IS), as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with Disaster Plan and Emergency Plan.

Controlled interface. A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).

Critical Design Review (CDR). A formal review conducted on each configuration item when design is complete. Determines that the design satisfies requirements, establishes detailed compatibility, assesses risk, and reviews preliminary product specifications.

Crypto-Ignition Key (CIK). A device or electronic key used to unlock the secure mode of crypto equipment.

Cryptologic Information System (IS). A Cryptologic IS is defined as any IS which directly or indirectly supports the cryptologic effort, to include support functions, such as, administrative and logistics, regardless of manning, location, classification, or original funding citation. This includes strategic, tactical, and support ISs; terrestrial, airborne, afloat, in-garrison, and spaceborne ISs; ISs dedicated to information handling; and information-handling portions of ISs that perform other functions.

Declassification (of IS Storage Media). An administrative action following sanitization of the IS or the storage media that the owner of the IS or media takes when the classification is lowered to unclassified. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities. The procedures for declassifying media require Designated Approving Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO) approval.

Defense Intelligence Agency (DIA). The Director, DIA is the authority for the promulgation of intelligence information systems (ISs) computer security policy, and is also the Principal Approving Authority (PAA) for the Security Accreditation against that policy of all ISs and networks processing, using, storing, or producing intelligence information.

Degauss. (1) To reduce the magnetization to zero by applying a reverse (coercive) magnetizing force commonly referred to as demagnetizing, or (2) to reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data. NOTE: A list of approved degaussers is updated and published quarterly in the "National Security Agency (NSA) Information Security Products and Services Catalog".

Department/Agency/Organization (DAO) Code. A 6-digit identification number assigned by the Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) Central Facility to organizational descriptions. The DAO code must be used by units when placing an order for STU-III/STE keying material.

Designated Approving Authority or Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system (or network) at an acceptable level of risk.

DAA Representative (DAA Rep). An official or service certification organization (SCO) responsible for ensuring conformance to prescribed security requirements for components of sites under their purview. SCOs are listed in the Department of Defense Intelligence Information Systems (DoDIIS) Information System Security Officer (ISSO) Handbook.

Destroying. Destroying is the process of physically damaging the media to the level that the media is not usable, and that there is no known method of retrieving the data.

Discretionary Access Control (DAC). A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

Diskette. A metal or plastic disk, coated with iron oxide, on which data are stored for use by an information system (IS). The disk is circular, rotates inside a square lubricated envelope that allows the read/write head access to the disk.

Department Of Defense (DoD) Intelligence Information Systems (DoDIIS). The aggregation of DoD personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence to military commanders and national level decision makers. For the purpose of this document, DoDIIS encompasses the Military Services, Defense Agencies, Defense Activities, Offices of the Secretary and Assistant Secretaries of Defense, the Organization of the Joint Chiefs of Staff, and the Unified Commands.

DoDIIS Site. An administrative grouping of a combination of Department of Defense Intelligence Information Systems (DoDIIS) accredited and managed collectively on the basis of geographical or organizational boundaries. Each DoDIIS Site contains multiple DoD intelligence information systems (ISs) which support the site's intelligence mission.

Fixed Disk. A magnetic storage device used for high volume data storage and retrieval purposes which is not removable from the disk drive in which it operates.

Flush. A computer program which is part of the Computer Security Toolbox. FLUSH is a MS-DOS based program used to eliminate appended data within a file or files and appended data located in unallocated or free space on a disk or diskette.

General User. A person accessing an information system (IS) by direct connections (e.g., via terminals) or indirect connections. NOTE: "Indirect connection" relates to persons who prepare input data or receive output that is not reviewed for content or classification by a responsible individual.

Government-Approved Facility. Any Government owned room or outside of a Sensitive Compartmented Information Facility (SCIF) with controlled or restricted access designed to limit public access which has operational procedures in place to actually limit access; any Government owned SCIF or area within a SCIF.

Guest system. Any system that enters the SCIF which has not already been certified or accredited by the respective cognizant SCIF authority is considered a Guest system.

Hard Disk. A magnetic storage device used for high volume data storage and retrieval purposes to include ones which are both removable and non-removable from the disk drives in which they operate.

Information Assurance. Information Operations that protect and defend data and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing restoration of IS by incorporating protection, detection, and reaction capabilities.

Information System (IS). Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice and/or data (digital or analog) and includes software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Information Systems (IS) and Network Security. IS and network security is the protection afforded to information systems in order to preserve the availability, integrity, and confidentiality of the systems and the information contained within the system. Such protection is the integrated application of communications security (COMSEC), TEMPEST, and information systems security (INFOSEC) executed in liaison with personnel security, operations security, industrial security, resources protection, and physical security.

Information Systems Security (INFOSEC). The protection of information systems (ISs) against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information Systems Security Engineer (ISSE). The person responsible for ensuring the security and integrity of a system during its life cycle and interfacing with other program elements to ensure security functions and safeguards are effectively integrated into the total system engineering effort. See SDSO.

Information Systems Security Manager (ISSM). The manager responsible for an organization's IS security program. Appointed by the Commander/Commanding Officer, the ISSM is the single point of contact for his/her organization concerning security matters to the Designated Approving Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO).

Information Systems Security Program Manager (ISSPM). The Air Force (AF) Air Intelligence Agency (AIA)/Army Intelligence and Security Command (INSCOM)/Navy Commander, Naval Security Group (COMNAVSECGRU) individual appointed by the Service Cryptologic Element (SCE) Commander/Commanding Officer as being the manager responsible for the SCE-level information systems (IS) and network security program and the security of all the agency's/command's ISs. Additionally, the ISSPM is the Designated Approving Authority (DAA) for the accreditation of systems on behalf of the NSA/CSS Senior Information Systems Security Program Manager (SISSPM).

Information Systems Security Officer (ISSO). The person responsible to the ISSM for ensuring that operational security is maintained for a specific IS, sometimes referred to as a Network Security Officer. Each organizational level unit assigns one ISSO per system. A ISSO may have the responsibility for more than one system. See System Administrator (SA).

Inspectable Space. A determination of the three-dimensional space surrounding equipment that processes classified and/or sensitive information within which TEMPEST exploitation is not considered practical, or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.

Integrity. Protection against unauthorized modification or destruction of information. Evident as an IS Security characteristic ensuring computer resources operate correctly and data in the system is accurate. This characteristic is applicable to hardware, software, firmware, and the databases used by the computer system.

Intelligence Community. A term which, in the aggregate, refers to the following Executive Branch organizations and activities: the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); offices within the Department of Defense; and others organized for collection of specialized national foreign intelligence through reconnaissance programs.

Interconnected System. A set of separately accredited systems that are connected together.

Interim Approval To Operate (IATO). Temporary authorization granted by a Designated Approving Authority (DAA) Representative (Rep)/Service Certifying Organization (SCO) for an information system (IS) to process classified information in its operational environment based on preliminary results of a security evaluation of the system.

Interoperability. The capability of one system to communicate with another system through common protocols.

Initial Operating Capability (IOC). A time when the persons in authority (e.g. program/project managers [PMs] or operations personnel) declare that a system meets enough requirements to formally be declared operational while the system may not meet all of the original design specifications to be declared fully operational.

Key Material Identification Number (KMID). A unique number automatically assigned to each piece of Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) keying material by the STU-III/STE.

Laptop. See Portable Computer System.

Level of Concern. The Level of Concern is a rating assigned to an IS by the DAA. A separate Level of Concern is assigned to each IS for confidentiality, integrity and availability. The Level of Concern for confidentiality, integrity, and availability can be Basic, Medium, or High. The Level of Concern assigned to an IS for confidentiality is based on the sensitivity of the information it maintains, processes and transmits. The Level of Concern assigned to an IS for integrity is based on the degree of resistance to unauthorized modifications. The Level of Concern assigned to an IS for availability is based on the needed availability of the information maintained, processed, and transmitted by the systems for mission accomplishment, and how much tolerance for delay is allowed.

Limited Release. A procedure to be used by United States SIGINT System (USSS) activities to control the release of storage media devices that have contained classified information to other activities outside the USSS community.

Local Area Network (LAN). Any local area capability to provide interoperability. See network.

Logic Bomb. A logic bomb is a program or code fragment which triggers an unauthorized, malicious act when some predefined condition occurs. The most common type is the "time bomb", which is programmed to trigger an unauthorized or damaging act long after the bomb is "set". For example, a logic bomb may check the system date each day until it encounters the specified trigger date and then executes code that carries out its hidden mission. Because of the built-in delay, a logic bomb virus is particularly dangerous because it can infect numerous generations of backup copies of data and software before its existence is discovered.

Malicious Code. Software or firmware that is designed with the intent of having some adverse impact on the confidentiality, integrity, or availability of an IS. It may be included in hardware, software, firmware or data. Computer Viruses, Worms, Trojan Horses, Trapdoors, and Logic/Time Bombs all fall under the definition of malicious code. Computer viruses pose the primary threat to ISs because of their reproductive capability.

Malicious Code Screening. Screening is the process of monitoring for the presence of malicious code. Malicious code occurs in different forms, which may have different methods for screening. Malicious code can arrive through either media that are introduced to IS or as mobile code that arrives through connections to other systems and networks.

Master Crypto-Ignition Key (CIK) Custodian. An individual at each node in a Community of Interest (COI) who is responsible for controlling and maintaining the Master CIK and programming the security features of the Secure Telephone Unit (STU)-III/STE.

Mission-Essential. In the context of information, that information which is an essential portion of a unit's mandatory wartime capability.

Mobile Code. The code obtained from remote systems, transmitted across a network, and then downloaded onto and executed on a local system. Mobile code has come to refer to web-based code downloaded onto a user's client and run by the user's browser. The larger set of mobile code normally involves an explicit decision to execute -- either by the user (manually) or by an application -- and an implicit decision autonomously made by an application.

Modem. A device that electronically Modulates and Demodulates signals, hence the abbreviation MODEM.

National Security Agency/Central Security Service (NSA/CSS). The Director, NSA/CSS is the authority for promulgation of computer security policy, and is also the Principal Approving Authority (PAA) for the security accreditation against that policy of all information systems (ISs) and networks processing, using, storing, or producing cryptologic information.

National Security Information (NSI). Information that has been determined, pursuant to Executive Order (EO) 12958 or any predecessor order, to require protection against unauthorized disclosure, and that is so designated.

National Security-Related Information. Unclassified information related to national defense or foreign relations of the United States.

Need-to-Know. A determination made by an authorized holder of classified information that a prospective recipient of information requires access to specific classified information to perform or assist in a lawful and authorized Government function, such as that required to carry out official duties.

Network. A combination of information transfer resources devoted to the interconnection of two or more distinct devices, systems, or gateways.

Network Manager. The individual who has supervisory or management responsibility for an organization, activity, or functional area that owns or operates a network.

Network Security Officer (NSO). An Individual formally appointed by a Designated Approving Authority (DAA)/Service Certifying Organization (SCO) to ensure that the provisions of all applicable directives are implemented throughout the life cycle of an information system (IS) network.

Network System. A system that is implemented with a collection of interconnected network components. A network system is based on a coherent security architecture and design.

Non-Volatile Memory Components. Memory components which DO RETAIN data when all power sources are disconnected.

Notebook. See Portable Computer System.

Object Reuse. Reassignment of a storage medium (e.g., page frame, disk sector, or magnetic tape) that contained one or more objects, after ensuring that no residual data remained on the storage medium.

Optical Storage Media. Optical mass storage, including compact disks (CD, CDE, CDR, CDROM), optical disks (DVD), and magneto-optical disks (MO)

Orange Book. Synonymous with the Department of Defense (DoD) Trusted Computer System Evaluation Criteria, DoD 5200.28-STD.

Organizational-level Commander/Commanding Officer. The individual, regardless of rank, which has been appointed as the officer-in-command of a physical organization.

Overwrite Procedure (for purposes of downgrading in limited cases). Process which removes or destroys data recorded on an information system (IS) storage medium by writing patterns of data over, or on top of, the data stored on the medium.

Overwrite Verification Procedure. A visual validation procedure that provides for reviewing, displaying, or sampling the level of success of an overwrite procedure.

Palmtop. See Portable Computer System.

Pass Phrase. Sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length.

Password. Protected/private character string used to authenticate an identity or to authorize access to data.

Password Shadowing. The ability within any operating system which physically stores the password and/or encrypted password results in a mass storage area of the system other than the actual password file itself. This feature prevents the theft of passwords by hackers. Usually a UNIX feature.

Periods Processing. The processing of various levels of classified and unclassified information at distinctly different times. Under the concept of periods processing, the system must be cleared of all information from one processing period before transitioning to the next. A system is said to operate in a "Periods Processing" environment if the system is appropriately sanitized between operations in differing protection level periods, or with differing user communities or data.

Peripheral. Any devices which are part of an information system (IS), such as printers, hard and floppy disk drives, and video display terminals.

Personal Digital Assistants (PDA)/Diaries (PDD). These items are mini processors with computing power that are generally smaller than laptop, notebook, or palmtop computers. Some examples include, but are not limited to, the Newton, Boss, Wizard, etc.

Phonemes. A phonetic word which sounds similar to an actual word. (Example, "fone" for "phone," "lafter" for "laughter").

Portable Computer System. Any computer system specifically designed for portability and to be hand carried by an individual (e.g., Grid, Laptop, Notebook, Palmtop, etc.).

Principal Accrediting Authority (PAA). The senior official having the authority and responsibility for all IS within an agency. Within the intelligence community, the PAAs are the DCI, EXDIR/CIA, AS/DOS (Intelligence and research), DIRNSA, DIRDIA, ADJC/FBI (National Security Div.), D/Office of Intelligence/DOE, SAS/Treasury (National Security), D/NIMA and the D/NRO.

Privacy (Not Security). The rights of an individual or organizations to determine for themselves when, how, and to what extent information about them is to transmitted to others.

Privileged User. The user of an information system (IS) who has root user authority.

Project/Program Manager (PM). The single individual responsible for a project or program who manages all day-to-day aspects of the project or program.

Protected Distribution System (PDS). A wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Protocols. Set of rules and formats, semantic and syntactic, that permits entities to exchange information.

Purge. The removal of data from an information system (IS), its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. Note: An IS must be disconnected from any external network before a purge. See Clearing.

RED. A designation applied to telecommunications and information systems (ISs), plus associated areas, circuits, components, and equipment which, when classified plain text signals are being processed therein, require protection during electrical transmission.

Red/Black Concept. Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form.

Remote Maintenance. An operational procedure that involves connection of a system to an external (i.e., outside of the facility securing the system), remote service for analysis or maintenance.

Removable Hard Disk. A hard disk contained in a removable cartridge type casing.

Risk Analysis. Synonymous with Risk Assessment.

Risk Assessment. Process of analyzing threats to and vulnerabilities of an information system (IS), and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

Risk Management. The discipline of identifying and measuring security risks associated with an IS, and controlling and reducing those risks to an acceptable level.

Routine Changes. Changes which have a minimal effect on the overall TEMPEST security of the Sensitive Compartmented Information (SCI) Facility (SCIF). Adding a different type of electronic information processing equipment (unless the equipment added is known to have an unusually large TEMPEST profile), movement of the equipment within the facility, and minor installation changes are examples of routine changes.

Sanitizing (Also Purging). The removal of information from media or equipment such that the data recovery using any known technique or analysis is prevented, as well as the removal of all classified labels and markings. Sanitizing allows moving the media to an environment with lower protection requirements. In general, laboratory techniques cannot retrieve data that has been sanitized/purged.

Sealed Disk Drive. See "Hard Disk".

Secure Copy. A computer program which is part of the Computer Security Toolbox. Secure Copy (SCOPY) is a MS-DOS based program used to eliminate appended data within a file or files while transferring the same from a source disk or diskette to a target disk or diskette.

Secure Data Device (SDD). The SDD provides a simple and cost-effective way to protect classified Government data transmissions. The SDD provides Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) secure data transmission functions without voice features and is fully interoperable with all other STU-III/STE products. It allows the user to access a computer database, send a facsimile (FAX) message, or use electronic mail and be sure the information is protected. The SDD was developed under the U.S. Government's STU-III/STE program and is approved for use by Federal departments, agencies, and Government contractors.

Secure Telephone Unit III (STU-III). The STU-III family includes several interoperable terminals capable of transmitting voice and data through the public telephone network. The STU-III can be used as an ordinary telephone, and can also be used as a secure terminal, connected through the public telephone network to other STU-IIIs. A STU-III Secure Data Device (SDD) provides STU-III secure data transmission functions without voice features. STU-IIIs are endorsed by the National Security Agency (NSA) for protecting classified or sensitive, unclassified U.S. Government information, when appropriately keyed.

Security. The protection of information to assure it is not accidentally or intentionally disclosed to unauthorized personnel.

Security Environment Changes. Changes which have a detrimental effect on the facility. Changes to the inspectable space (IS), addition of a radio transmitter or a modem for external communications, removal or reduction of an existing TEMPEST countermeasure (Radio Frequency Interference [RFI] Shielding, Filters, Control/Inspectable space, etc.) would be changes to the security environment.

Security Testing. The process to determine that an information system (IS) protects data and maintains functionality as intended.

Security Training, Education and Motivation (STEM). A security education program designed to educate and motivate personnel concerning the protection of priority resources and the safeguarding of classified information.

Senior Information Systems Security Program Manager (SISSPM). The national-level individual appointed by the Director, National Security Agency (DIRNSA) as being the manager responsible for the national-level Service Cryptologic Element (SCE) Information Systems (IS) and Network Security Program, the security of all Cryptologic ISs, and is the Designated Approving Authority (DAA) for the accreditation of systems on behalf of the DIRNSA.

Senior Intelligence Officer (SIO). The highest ranking military or civilian individual charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, or element of an intelligence community organization or Department of Defense (DoD) Intelligence Activity assigned responsibilities or designated authorities by a Senior Official of the Intelligence Community (SOIC).

Senior Officials of the Intelligence Community (SOIC). The heads of organizations or their designated representatives within the Intelligence Community, as defined by Executive Order (EO) 12333.

Sensitive But Unclassified (SBU) Information. Information collected, maintained, and/or disseminated by an agency that is not classified but whose unauthorized release or use could compromise or damage privacy or proprietary rights, critical agency decision making, and/or the enforcement or implementation of public law or regulations under which the agency operates.

Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCID 1/19).

Sensitive Compartmented Information (SCI) Facility (SCIF). An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed and/or electronically processed.

Service Certifying Organization (SCO). The organization responsible for ensuring conformance to prescribed security requirements for components of sites under their purview. SCOs are listed in the Department of Defense Intelligence Information Systems (DoDIIS) Information System Security Officer (ISSO) Handbook.

Service Cryptologic Elements (SCE). A term used to designate, separately or together, those elements of the U.S. Army, Navy, and Air Force which perform cryptologic functions. The Air Force Air Intelligence Agency (AIA), Army Intelligence and Security Command (INSCOM), and Navy Commander Naval Security Group (COMNAVSECGRU) are the SCEs responsible to the National Security Agency/Central Security Service (NSA/CSS) for accreditation of all cryptologic information systems (ISs) within their respective services.

Site Information Systems Security Manager (Site ISSM). The single information systems (IS) security focal point for a defined site. The site ISSM supports two organizations: User organization and technical organization. The site ISSM is responsible for managing the baseline and ensuring that changes to the site baseline are properly controlled.

Site Integration Management Office (SIMO). The major functions of the SIMO are: Establishing baselines, monitoring compliance, configuration management, and integration transition. There are three levels of such offices: DoDIIS, Service, and site. Only the larger sites will have a site SIMO.

Special Access Program (SAP). Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine "need-to-know"; or special lists of persons determined to have a "need-to-know".

Special Security Officer (SSO). The individual assigned responsibility for the security management, operation, implementation, use and dissemination of all Sensitive Compartmented Information (SCI) material within his/her respective organization.

Stand-Alone System. An information system (IS) operating independent of any other IS within an environment physically secured commensurate with the highest classification of material processed or stored thereon.

Survivability. The capability of a system to withstand a man-made or natural hostile environment without suffering an abortive impairment of its ability to accomplish its dedicated mission.

SYSOP. An operator responsible for performing system-oriented procedures. See System Administrator.

System. A generic name for an Information System (IS).

System Administrator (SA). The individual responsible for maintaining the system in day-to-day operations. The SA has responsibility to: manage system hardware and software, data storage devices and application software; manage system performance; provide system security and customer support; perform equipment custodian duties; maintain software licenses and documentation; monitor hardware and software maintenance contracts; establish USERIDs and passwords; ensure adequate network connectivity; review audit trails; and provide backup of system operations and other system unique requirements. See Information System Security Officer (ISSO).

System Design Security Officer (SDSO). An individual responsible for ensuring that adequate security requirements are stated in the design specifications of new systems and system upgrades during the design phase of their life cycle. This individual works closely with all project/program acquisition managers. See ISSE.

System Security Engineering. The efforts that help achieve maximum security and survivability of a system during its life cycle and interfacing with other program elements to ensure security functions are effectively integrated into the total system engineering effort.

System Security Authorization Agreement (SSAA). A formal document that fully describes the planned security tasks required to meet system or network security requirements. The package must contain all information necessary to allow the DAA Rep/SCO to make an official management determination for authorization for a system, network, or site to operate in a particular security mode of operation; with a prescribed set of safeguards, against a defined threat with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnections to external systems; and at an acceptable level of risk.

System Security Plan (SSP). See System Security Authorization Agreement.

Technical Vulnerability. A hardware, firmware, communication, or software weakness which leaves an information system (IS) open for potential exploitation or damage, either externally or internally resulting in risk for the owner, user, or manager of the IS.

TEMPEST. A short name referring to investigation, study, and control of compromising emanations from telecommunications and information system (IS) equipment. TEMPEST must be considered during all life cycle phases of equipment. (See Compromising Emanations).

TEMPEST Approved. This term applies to equipment or systems which have been built and certified to meet Level I of National Security Telecommunications Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements.

TEMPEST Zone. A defined area within a facility where equipment with appropriate TEMPEST characteristics (TEMPEST zone assignment) may be operated without emanating electromagnetic radiation beyond the controlled space boundary of the facility.

TEMPEST Zoned Equipment. Equipment that has been evaluated and assigned an equipment zone corresponding to the level in National Security Telecommunications Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92. This equipment must be installed according to the NSTISSAM and HQ-Level specialized installation instructions.

Terminal Area. A subset or part of the overall work space assigned to a specific area within an organization. An area within the typical office environment restrictive in size such that it permits one person to observe and monitor access with the intent of preventing Information System (IS) abuse and unauthorized IS access.

Threat Assessment. The process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Threat Monitoring. The analysis, assessment, and review of Information Systems (ISs) audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of data or system security.

Toolbox. See Computer Security Toolbox.

Trapdoor. Operating system and application safeguards that usually prevent unauthorized personnel from accessing or modifying programs. During software development, however, these built-in security measures are usually bypassed. Programmers often create entry points into a program for debugging and/or insertion of new code at a later date. These entry points (trapdoors) are usually eliminated in the final stages of program development, but they are sometimes overlooked, accidentally or intentionally. A perfect example of a trapdoor was dramatized in the movie War Games, where the teen-age hacker enters the special password "Joshua" and gains unrestricted access to a mainframe computer in NORAD headquarters. Such a mechanism in a computer's operating system can grant an attacker unlimited and virtually undetectable access to any system resource after presenting a relatively trivial control sequence or password.

Trojan Horse. A computer program containing an apparent or actual useful function that contains additional (hidden) functions that allows unauthorized collection, falsification, or destruction of data. This is the most commonly used method for program-based frauds and sabotage.

Trusted Computing Base (TCB). The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. NOTE: The ability of a TCB to enforce correctly a unified security policy depends on the correctness of the mechanisms within the TCB, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

Trusted Path. A mechanism by which a person using a terminal can communicate directly with the trusted computing base (TCB). **NOTE:** The trusted path can only be activated by the person or the TCB and cannot be initiated by untrusted software.

uNclassified Internet Protocol Router NETwork. The unclassified network which replaced the military unclassified network. Provides connection to the world wide web.

Unclassified Sensitive. For computer applications, this term refers to any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under the criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Computer Security Act of 1987, Public Law 100-235). Also see Sensitive but Unclassified (SBU) Information.

User Identification (USERID). A unique symbol or character string that is used by an information system (IS) to uniquely identify a specific user.

User Network Manager (UNM). Each sponsor of a Community-of-Interest (COI) must designate an individual who will be responsible for the management of the network, request permission to use the data port, and ensure compliance with the security procedures defined in appropriate security policy documents and those specifically defined in the approval process.

User Representative (UR). A person formally designated, on behalf of the Command Authority, who is responsible for preparing and submitting all key orders (including Sensitive Compartmented Information [SCI]) to the Central Facility. The UR has the responsibility for monitoring the status of those orders, to include keeping the Communications Security (COMSEC) manager informed of the pending key request in situations where the UR is other than the COMSEC manager.

Virus. A self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

Volatile Memory. Random Access Memory (RAM) which is not retained upon system shutdown.

Vulnerability. A weakness in an information system (IS), or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls), that could be exploited.

Wide Area Network (WAN). A computer network that services a large area. WANs typically span large areas (states, countries, and continents) and are owned by multiple organizations. See Local Area Network and Network.

Worm. A worm is a program, originally developed by systems programmers, which allows the user to tap unused network resources to run large computer programs. The worm would search the network for idle computing resources and use them to execute a program in small segments. Built-in mechanisms would be responsible for maintaining the worm, finding free machines, and replicating the program. Worms can tie up all the computing resources on a network and essentially shut it down. A worm is normally activated every time the system is booted up. This is differentiated from WORM (write-once, read many) descriptive of optical (compact disk) media with single write capability.

Write Protect. A term used to indicate that there is a machine hardware capability which may be manually used to protect some storage media from accidental or unintentional overwrite by inhibiting the write capability of the system. (For example, write protection of magnetic tapes is accomplished by the physical removal of the "write-ring" from the back of the tape. Write protection of three and one half inch floppy diskettes refers to the correct placement of the sliding tab to the open position which inhibits the hardware capability to perform a physical write to the diskette. Write protection includes using optical disks within CD read-only devices.)

APPENDIX C

SUMMARY OF CHANGES

SORT: 1400.34
DOCI: DODD 1400.34
DATE: 19881215
TITL: DODD 1400.34 DoD Civilian **Intelligence** Personnel Management System (CIPMS), December 15, 1988, ASD(FM&P), thru change 2, November 16, 1994

Refs: (a) Title 10, United States Code, Chapter 81, Section 1590
(b) DoD Directive 5010.10, "**Intelligence** Career Development Program," August 9, 1972

A. PURPOSE

This Directive:

1. Implements reference (a).

2. Establishes policy, assigns responsibilities, and provides guidance for the DoD Civilian **Intelligence** Personnel Management System (CIPMS).

3. Authorizes the publication of DoD 1400.34-M, "DoD Civilian **Intelligence** Personnel Management System (CIPMS) Procedures."

B. APPLICABILITY

This Directive applies to all civilian employees within those commands and activities that have a primary **intelligence** mission and to those who perform related work in nonintelligence commands and activities of the Military Departments. Law enforcement officials are not included.

C. DEFINITIONS

1. Activity. Separate organizational components at various levels of command within a Military Department.

2. Executive Secretary. Designated by the Assistant Secretary of Defense (Force Management and Personnel) (ASD(FM&P)) to assist in the administration of the CIPMS.

3. Functional Chief. The Senior Military **Intelligence** Officer (SIO) of each Military Department.

D. POLICY

It is DoD policy that:

1. The CIPMS shall operate as the single personnel management system for personnel described in section B. The CIPMS goal is to improve the acquisition, professional development, and long-term retention of a quality civilian work force within the military **intelligence** community, and to have functional management directly involved in all aspects of program development, administration, and evaluation. Conversion of employees to the CIPMS shall begin immediately, but may be accomplished through occupational phasing.

2. The CIPMS shall include:

a. Use of the CIPMS primary grading standards, occupational guides, career paths and ladders, grade bands or career levels, and special consideration of the impact of the person on the job in the grading of positions.

b. Classification appeal decision authority within each Military Department.

c. Direct appointing authority as delegated by the Secretary of Defense.

d. A single DoD system for pay and allowances that provides for special CIPMS salary rates and overseas entitlements.

e. A general framework for DoD-wide CIPMS program evaluation.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense (Force Management and Personnel) (ASD(FM&P)) shall:

a. In coordination with the Assistant Secretary of Defense (Command, Control, Communications and **Intelligence**) (ASD(C3I)), interpret legislation relating to the CIPMS.

b. Develop, approve, and publish DoD-level CIPMS policy and procedures.

c. Establish and manage a CIPMS Advisory Group and appoint an Executive Secretary.

2. The Assistant Secretary of Defense (Command, Control, Communications and **Intelligence**) (ASD(C3I)) shall:

a. Determine and provide to the ASD(FM&P) **intelligence** mission goals and objectives for use in developing the CIPMS policy and procedures, and ensure program evaluation in accordance with DoD Directive 5010.10 (reference (b)).

b. Coordinate on all proposed and revised CIPMS regulations, policy, procedures, and standards.

c. Provide a representative to the CIPMS Advisory Group.

d. Recommend to the ASD(FM&P) exceptions to the employee coverage of the CIPMS.

3. The Secretaries of the Military Departments shall:

a. Implement and administer the CIPMS and develop supplemental regulations to satisfy specialized departmental needs.

b. Use their discretion to include in the CIPMS those employees in direct support of **intelligence** functions located in nonintelligence commands, activities, and organizations.

c. Begin conversion of covered employees to the CIPMS upon the effective date of this Directive. If a phased implementation approach is used, the plan shall be described in the implementing documents.

d. Terminate the employment of any CIPMS employee when such action is considered to be in the interest of the United States and when procedures prescribed in other statutes cannot be invoked in a manner consistent with the national security.

e. Comply with the **Intelligence** Career Development Program (ICDP) (DoD Directive 5010.10, reference (b)).

4. The Functional Chiefs of the Military Departments shall:

a. Coordinate on implementing regulations, policy, procedures, and standards for the CIPMS.

b. Participate in program evaluation in accordance with responsibilities prescribed in reference (b).

F. EFFECTIVE DATE

This Directive is effective immediately.

William H. Taft, IV Deputy Secretary of Defense

Department of Defense

DIRECTIVE

NUMBER 3150.5

March 24, 1987

ASD(ISA)

SUBJECT: DoD Response to Improvised Nuclear Device (IND) Incidents

References: (a) DoD Directive 3150.5, "DoD Response to Improvised Nuclear Device Threats," July 19, 1985 (hereby canceled)

(b) "Joint Federal Bureau of Investigation, Department of Energy and Department of Defense Agreement for Response to Improvised Nuclear Device Incidents," February 27, 1980

(c) "Joint Department of State, Department of Energy and DoD Memorandum of Understanding for Responding to Malevolent Nuclear Threats Outside U.S. Territory and Possessions," January 28, 1982

(d) DoD Directive 3025.12, "Employment of Military Resources in the Event of Civil Disturbances," August 19, 1971

(e) through (i), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policies and procedures for the DoD response to IND incidents, to implement the DoD technical responsibilities defined in references (b) and (c), and to amplify the direction concerning law enforcement and other associated responsibilities issued in reference (d) and DoD Directive 5100.46 (reference (e)).

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, the Defense Nuclear Agency (DNA), and the Defense Intelligence Agency (DIA). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.2. Assigns responsibilities and authorities for the following:

2.2.1. Command and control of DoD resources.

2.2.2. Operational response.

2.2.3. Requirements for research and development.

2.2.4. Participating in joint working groups, exercises, and activities.

2.2.5. Training of Explosive Ordnance Disposal (EOD) Forces.

2.3. Amplifies the DoD law enforcement responsibilities and authorities associated with an IND incident that are addressed in DoD Directive 3025.12 (reference (d)).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy to assist the lead Federal Agency during an IND incident. The Federal Bureau of Investigation (FBI) is the lead Federal Agency for IND incidents in U.S. territories and possessions. The Department of State (DoS) is the lead Agency for acts not under FBI responsibility. When the Department of Defense responds to an IND incident, operational control over DoD assets is exercised by the DoD senior representative.

5. RESPONSIBILITIES

The joint FBI, Department of Energy (DoE), DoD agreement and the joint DoS, DoE, DoD memorandum (references (b) and (c)) include procedures and responsibilities to be followed for IND incidents. DoD Instruction 5100.52 (reference (f)) provides guidance for accidents involving radioactive materials. Reference (d) and Directives 5100.46 and 3025.1 (references (e) and (g)) provide policy for military assistance to civil disturbances and foreign disasters. Consistent with this Directive and its references, Military Commanders remain responsible for the safety and security of military personnel and property. Nothing contained herein shall restrict the national security responsibilities of the Department of Defense.

5.1. The Secretary of the Army, the Secretary of the Navy, and the Secretary of the Air Force shall:

5.1.1. In accordance with this Directive, provide resources to address responsibilities in accordance with references (b) and (c).

5.1.2. Implement this Directive.

5.2. The Assistant Secretary of Defense (International Security Affairs) (ASD(ISA)) shall:

5.2.1. Act as DoD Executive Agent for establishing IND incident response policy and for providing guidance to the Services and DoD Agencies.

5.2.2. Coordinate interdepartmental exercises and operations.

5.2.3. Ensure that sufficient funds are budgeted by Services for maintaining operational response teams and for participating in interdepartmental exercises.

5.3. The Assistant to the Secretary of Defense (Atomic Energy) (ATSD(AE)) shall:

5.3.1. Provide the DoD representation to the DoE Nuclear Emergency Search Team (NEST) Executive Planning Board (NEPB) and the joint working groups.

5.3.2. Provide guidance on IND response training, equipment,

and research and development. Coordinate research and development with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)).

5.3.3. Approve DoD EOD research and development program for INDs and coordinate with DNA and DoE on research and development programs.

5.4. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) shall coordinate and support research and development of IND response capabilities.

5.5. The Assistant Secretary of Defense (Public Affairs) (ASD(PA)) shall provide the public affairs interface with other Government Agencies and shall provide public affairs guidance to the Services.

5.6. The Director, Defense intelligence Agency (DIA), shall collect and report intelligence information on foreign IND incidents.

5.7. The Director, Defense Nuclear Agency (DNA), shall:

5.7.1. Maintain an active relationship with and assist the Services, DoE, and other Agencies involved in IND countermeasures and response actions.

5.7.2. Participate in IND contingency planning meetings, joint working groups, DoE NEPB, Service, and other Federal Agency activities.

5.7.3. Provide response resource and capability information through the Joint Nuclear Accident Coordinating Center (JNACC).

5.7.4. When requested by a Service or Commander in Chief (CINC), provide the DoD Senior Representative for Continental United States (CONUS) incidents as well as other required DNA assets to support the response to the IND incident

5.7.5. Participate in the planning of IND exercises and training by facilitating DoD participation. Observe IND exercises and training to monitor interdepartmental and inter-Service coordination.

5.8. The Secretary of the Army shall:

5.8.1. Provide a trained response team of EOD personnel and other required support for responding to IND incidents on Army installations in the CONUS, the CONUS land mass (except for those installations specifically assigned as a responsibility of the Navy, Air Force, or Marine Corps), and other areas as directed by the National Command Authority (NCA) through the Joint Chiefs of Staff (JCS).

5.8.2. Submit IND countermeasures technology and training requirements to the Executive Manager for DoD Explosive Ordnance Disposal Technology and Training (EODT&T) in accordance with DoD 5160.62 (reference (h)).

5.8.3. Fund Army IND response team training, exercises, and operations.

5.8.4. Participate in joint working groups, NEST technical working groups, and interdepartmental exercises.

5.9. The Secretary of the Navy shall:

5.9.1. Provide a trained response team of EOD personnel and other required support for responding to IND incidents on Navy and Marine Corps CONUS installations, IND incidents

involving underwater threats, and other areas as directed by the NCA through the JCS.

5.9.2. Submit IND countermeasures technology and training requirements to the Executive Manager for EODT&T in accordance with reference (h).

5.9.3. Fund Navy IND response team training, exercise, and operations.

5.9.4. Participate in joint working groups, NEST technical working groups, and interdepartmental exercises.

5.9.5. Fund and perform research and development program for IND countermeasures, concentrating on access and disablement, which meets the requirements of all DoD Components and is approved by the ATSD(AE).

5.9.6. Establish and fund a Joint Service DoD Technical Response Group (DTRG) to provide specialized equipment and technical assistance to the response team.

5.9.7. Establish and fund joint Service IND countermeasures training and exercises based upon inputs from DoD Components.

5.9.8. Provide technical program support to the DoD NEPB representative and coordinate the DoD research and development (R&D) program with the DoE R&D program, joint working groups, and NEST technical working groups.

5.10. The Secretary of the Air Force shall:

5.10.1. Provide a trained response team of EOD personnel and other required support for responding to IND incidents on Air Force CONUS installations and other areas as directed by the NCA through the JCS.

5.10.2. Submit IND countermeasures technology and training requirements to the Executive Manager for EODT&T in accordance with reference (h).

5.10.3. Fund the Air Force IND response team training, exercises, and operations.

5.10.4. Participate in joint working groups, NEST technical working group, and interdepartmental exercises.

5.11. The Commanders of Unified Commands Outside Continental U.S. (OCONUS) shall:

5.11.1. Support Service-component trained response teams of EOD personnel when they are deployed to an OCONUS unified theater and provide other required support in response to IND incidents on installations and areas under their authority.

5.11.2. Submit IND countermeasures technology and training requirements to the Executive Manager for EODT&T.

5.11.3. Evaluate response team performance in exercises and operations.

5.12. The Military Airlift Command (MAC) shall plan for and provide Special Assignment Air Mission (SAAM) support for deployment of DoD and interdepartmental IND response teams.

5.13. The Chairman, Joint Chiefs of Staff (CJCS), shall:

5.13.1. In coordination with Services and appropriate Defense Agencies, be responsible for implementing the military response to an IND incident.

5.13.2. Notify the National Security Council (NSC), lead Federal Agency, DoE, and the Service or CINC Command

Center of IND incidents.

5.13.3. Keep the Secretary of Defense and OSD staff informed of the IND incident.

6. PROCEDURES

6.1. When the National Military Command Center (NMCC) is notified of an IND incident, the Operations Team shall notify the lead Federal Agency, the appropriate Service or CINC, and other appropriate Agencies.

6.2. The Operations Team within the NMCC shall interface with non DoD organizations and shall facilitate inter-Service support required for such operations. When the U.S. Government responds to an IND incident in a foreign country, the U.S. Ambassador shall coordinate U.S. response operations with the host government.

6.3. In U.S. territories and possessions, the FBI Senior Agent in Charge (SAC) shall be the senior U.S. Government official and shall coordinate and communicate with local authorities.

6.4. The DoD response team shall be prepared for deploying within 4 hours of notification of an IND incident. The DoD response team shall be under the command and control of the DoD senior representative, provided by the responsible Service or CINC, who shall establish coordination with the lead Federal Agency. In accordance with the joint agreement (reference (b)), the lead Federal Agency shall be responsible for establishing coordination with non-DoD response Agencies. The DoD response team shall establish secure communications, when possible, with the NMCC or the respective CINC and Service Command Center. The DoD Technical Response Group (DTRG) shall deploy at the discretion of the DoD senior representative or the NMCC.

6.5. The Services and CINCs shall fund incurred costs of operational deployments under this Directive and the joint agreement and joint memorandum (references (b) and (c)). Subsequent reimbursements shall be in accordance with DoD Directive 5100.46 (reference (e)) and 31 U.S.C. 1535 (reference (i)).

7. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of the implementing document to the Assistant Secretary of Defense (International Security Affairs) within 120 days.

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Directive 5100.46, "Foreign Disaster Relief," December 4, 1975

(f) DoD Instruction 5100.52, "Radiological Assistance in the Event of an Accident Involving Radioactive Materials," March 10, 1981

(g) DoD Directive 3025.1, "Use of Military Resources during Peacetime Civil Emergencies within the United States, its Territories and Possessions," May 23, 1980

(h) DoD Directive 5160.62, "Single Manager Assignment

for Military Explosive Ordnance Disposal Technology
and Training (EODT&T)," November 24, 1971

(i) Section 1535 of title 31, United States Code

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. DoD Response Team. A DoD organization, trained, exercised, and equipped to assist the lead Federal Agency in response to IND incidents.

E2.1.2. DoD Senior Representative. The DoD official, provided by the responsible Service or CINC, who directs the DoD response team at the scene of an IND incident, advises the lead Federal Agency, coordinates operations with the DoE on-site technical teams, and has the authority to request additional DoD resources.

E2.1.3. DoD Technical Response Group (DTRG). A trained joint Service EOD advisory group consisting of scientific and technical personnel trained and equipped for supporting and assisting the operational response teams.

E2.1.4. Explosive Ordnance Disposal (EOD). The detection, identification, field evaluation, rendering-safe, recovery, neutralization, and final disposal of unexploded explosive ordnance (UXO) including nuclear, chemical, biological, and improvised explosive ordnance.

E2.1.5. Explosive Ordnance Disposal Program Board (EODPB). The organization that acts in an advisory capacity to the Executive Manager, EOD Technology and Training (EODT&T), comprising a representative from each of the Military Departments.

E2.1.6. Improvised Nuclear Device (IND). A device incorporating radioactive materials designed to result in the dispersal of radioactive material or in the formation of a nuclear-yield reaction. Such devices may be fabricated in a completely improvised manner or may be an improvised modification to a U.S. or foreign nuclear weapon.

E2.1.7. Joint Nuclear Accident Coordinating Center (JNACC). A combined DNA and DoE centralized Agency for exchanging and maintaining information concerned with radiological assistance capabilities and coordinating assistance activities.

E2.1.8. Lead Federal Agency. In CONUS and in U.S. territories and possessions, the lead Federal Agency is the FBI. In areas not under FBI jurisdiction, the DoS is the lead Federal Agency.

E2.1.9. National Military Command Center (NMCC). Centralized controlling and notifying point for activating and coordinating DoD activities.

E2.1.10. Nuclear Emergency Search Team (NEST). A DoE chartered group of scientists, engineers, and technicians with specialized equipment and procedures for providing technical assistance at the scene of a IND incident.

E2.1.11. Nuclear Emergency Search Team Executive Planning Board (NEPB). The organization reporting to the DoE manager of the Nevada Operations Office comprising top executives from each of the contributing laboratories, Agencies, and contractors that supports NEST activities. The NEPB's primary objective is to establish criteria and provide recommendations for the DoE NEST program.

SORT: 3305.5

DOCI: DODD 3305.5

DATE: 19860509

TITL: DODD 3305.5 General Defense **Intelligence** Program (GDIP) Management, May 9, 1986, ASD(C3I)

Refs:(a) Title 10, United States Code, Section 133

(b) Assistant Secretary of Defense (Command, Control, Communi cations and **Intelligence**) Memorandum, "Management of General **Intelligence** Resources," July 28, 1977 (hereby canceled)

(c) Executive Order 12333, "United States **Intelligence** Activities," December 4, 1981

(d) DoD Directive 5105.21, "Defense **Intelligence** Agency," May 19, 1977

(e) DoD Directive 5137.1, "Assistant Secretary of Defense (Command, Control, Communications, and **Intelligence**)," April 2, 1985 (f) DoD Directive 5000.19, "Policies for the Management and Control of Information Requirements," March 12, 1976

A. PURPOSE

This Directive:

1. Designates the Director, Defense **Intelligence** Agency (DIA), as Program Manager of the General Defense **Intelligence** Program (GDIP) and establishes a GDIP Staff to support the Program Manager, pursuant to the authority vested in the Secretary of Defense under reference (a).

2. Supersedes reference (b).

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components"). The term "Military Services," as used herein, refers to the Army, Navy, Air Force, and Marine Corps.

C. DEFINITION

The General Defense **Intelligence** Program is part of the National Foreign **Intelligence** Program (NFIP) as defined in Section 3.4(g) of reference (c). It includes those national **intelligence** activities of the Department of Defense that are not in other NFIP components. The GDIP includes specialized national reconnaissance sub systems and communications **intelligence** components of multisensor systems. It may include other National Foreign **Intelligence** Program activities as agreed between the Secretary of Defense and the Director of Central **Intelligence** (DCI).

D. RESPONSIBILITIES

The Director, Defense **Intelligence** Agency, in addition to discharging the responsibilities and functions assigned in DoD Directive 5105.21 (reference as GDIP Manager, shall centrally manage the resource planning, programming and budgeting of the NFlP resources of the Department of Defense that are not included in other NFIP components and shall:

1. Ensure that the activities of the GDIP support national and DoD **intelligence** goals, objectives, and priorities identified by the DCI and the Secretary of Defense; the requirements of the Joint Chiefs of Staff (JCS) and of the Unified and Specified Commands validated by the JCS and the missions of the Military Departments.

2. Respond to DCl guidance, and develop and submit to the DCl proposed programs and budgets in the format designated by the DCI.

3. Provide the DCl with all information concerning the GDIP and its component elements necessary for the DCI to implement program and budget responsibilities assigned in E.O. 12333 (reference (c)).

4. Respond to Secretary of Defense guidance, and provide the Assistant Secretary of Defense (Command, Control, Communications, and **Intelligence**) (ASD(C3I)) with all information concerning the GDIP and its component elements necessary to accomplish the functions and responsibilities stated in DoD Directive 5137.1 (reference (e)).

5. To ensure support of DoD elements' priorities and objectives, at critical points during development of the program conduct reviews and evaluations with participation of senior representatives of OJCS, the Unified and Specified Commands, the Military Services, and the ASD(C3I).

6. Work closely with the ASD(C3I) and staff in accordance with reference (e) to ensure maximum complementarity and mutual support among the GDIP and other DoD **intelligence** programs, and to ensure that the GDIP is based on validated requirements.

7. Exercise responsibility for GDIP resource planning, guidance, programming, and budgeting, and shall:

a. Provide program policy guidance and instructions for DIA and Military Department resource planning, programming, and budgeting.

b. Make program and budget recommendations to the ASD(C3I) in accordance with reference (e).

c. Task GDIP components, as required, to support GDIP program management responsibilities and to respond to DCI, OSD, Office of Management and Budget (OMB), and Congress on GDIP matters.

d. Produce congressional budget justifications and represent GDIP components and activities during congressional program/budget authorization and appropriation hearings and reviews dealing with GDIP matters.

e. Identify and resolve GDIP-related program, budget, and management issues and problems.

f. Monitor the DoD budget to ensure that DCI resource decisions concerning the GDIP are accurately reflected; and identify issues arising therefrom to the ASD)(C3I) or the Assistant Secretary of Defense (Comptroller) (ASD(C)) for resolution.

g. Coordinate, as appropriate, GDIP planning guidance, resource plans, programs, and proposed budgets with other national foreign **intelligence**, DoD and Military Department **intelligence** and **intelligence**-related programs and budgets.

h. Assess the effectiveness of GDIP programs and activities; their responsiveness to identified national, DoD, and Unified and Specified Command needs; and the adequacy of interrelationships between GDIP activities and those of other **intelligence** and **intelligence**-related programs.

8. Designate an Acting Program Manager in the Program Manager's absence.

E. GENERAL DEFENSE **INTELLIGENCE** PROGRAM STAFF

1. The GDIP Program Manager shall be supported by a directly subordinate GDIP Staff. The GDIP Staff shall operate independently of the DIA, but within the authorities assigned to the Director of DIA in this Directive and in DoD Directive 5105.21 (reference (d)). Except as otherwise provided by agreement between the Program Manager and other offices and agencies, the DIA shall provide the GDIP Staff with administrative, logistical, personnel, financial, and other support.

2. The GDIP Staff shall be headed by a Director who shall function as the Deputy Program Manager and program coordinator. The Deputy Program Managershall exercise such responsibilities and functions as the Program Manager delegates.

3. Members of the GDIP Staff shall represent the Program Manager, as appropriate, in contacts with other elements of the Department of Defense, OMB, the **intelligence** community, and congressional staffs.

4. The GDIP Staff shall develop and produce documents such as the annual Program Manager'S Guidance Memorandum, the GDIP Budget Forecast, and the GDIP Budget Estimate to implement the Program Manager's responsibilities.

F. AUTHORITIES

The administrative authorities required by the Director, DIA, to administer and direct the operation of the DIA, as stated in the enclosure to DoD Directive 5105.21 (reference (d)), are hereby delegated to the GDIP Program Manager to administer and direct the operations of the GDIP Staff. In performing the assigned responsibilities and functions relating to the GDIP, the Program Manager is specifically delegated authority to:

1. Establish, operate, and control the GDIP Staff and its activities.

2. Assign tasks and issue instructions and guidance to the DoD elements of the GDIP as necessary to carry out the GDIP management responsibilities. This delegation of authority enabled the GDIP Manager to deal directly with the Military Departments on GDIP matters.

3. Have free and direct access to and communicate with DoD Components, agencies within the U.S. **Intelligence** Community, and other executive departments and agencies, as necessary.

4. Obtain from any DoD Component such information as may be necessary to perform assigned functions, subject to DoD Directive 5000.19 (reference (f)).

5. Enter into intra-Department of Defense and interagency agreements and understandings, as necessary, for GDIP management and determination of resource requirements of GDIP units and activities.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. The GDIP Program Manager shall issue implementing documents within 90 days.

William H. Taft, IV Deputy Secretary of Defense

SORT: 4630.05
DOCI: DODD 4630.5
DATE: 19921112
TITL: DODD 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and **Intelligence** (C3I) Systems, November 12, 1992, ASD(C3I)

Refs: (a) DoD Directive 4630.5, "Compatibility and Interoperability of Tactical Command, Control, Communications, and **Intelligence** Systems," October 9, 1985 (hereby canceled)
(b) DoD Directive 5000.1, "Defense Acquisition," February 23, 1991
(c) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991
(d) Section 2457 of title 10, United States Code

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) and promulgates policy for compatibility, interoperability, and integration of C3I systems used in the Department of Defense.

B. APPLICABILITY AND SCOPE

This Directive applies to:

1. The Off ice of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2. All new C3I systems (including nondevelopmental systems) and major changes (e.g. release of a new software version) to existing systems that must interact with or be integrated into the C3I structures of the Department.

C. DEFINITION

Principal Staff Assistants. Undersecretaries of Defense, Assistant Secretaries of Defense, General Counsel of the Department of Defense, Inspector General of the Department of Defense, Comptroller of the Department of Defense, Assistants to the Secretary of Defense, and OSD Directors or equivalents who report directly to the Secretary or Deputy Secretary of Defense.

D. POLICY

It is DoD Policy:

1. That forces for joint and combined operations must be supported through compatible, interoperable, and integrated C3I systems that can support operations worldwide throughout the entire spectrum of conflict.

2. To establish as a long-term objective a DoD-wide, global C3I infrastructure that can accommodate the widest possible range of missions and operational scenarios by allowing users to enter the infrastructure at anytime, anyplace, in the execution of any mission.

3. In accordance with DoD Directive 5000.1 and DoD Instruction 5000.2 (references (b) and (c)), to develop, acquire, and deploy C3I systems and equipment that meet essential operational needs of U.S. forces, that are compatible with existing and planned C3I systems, and other electronic equipment, and that are interoperable with other U.S. and allied nations'

functionally related C3I information systems and equipment. See 10 U.S.C. 2457 (reference (d)), which establishes a policy of Standardization and interoperability within the North Atlantic Treaty Organization.

4. That, for purposes of compatibility, interoperability, and integration, all C3I systems developed for use by U.S. forces are considered to be for joint use.

5. That interoperability and integration of C3I requirements shall be determined during the requirements validation process and shall be updated as necessary throughout the acquisition period, deployment, and operational life of a system.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** shall assign responsibilities and prescribe procedures, as necessary, to ensure the policies outlined in section D., above, are carried out.

2. The Principal Staff Assistants shall, during all technical, program, budget, funding, or other reviews of the Military Departments or the Defense Agencies affecting compatibility and interoperability requirements, make recommendations to the appropriate decision authority about the conformance to the policies outlined in section D., above.

3. The Chairman of the Joint Chiefs of Staff shall:

a. In accordance with references (b) and (c), establish procedures for the development, coordination, review, and validation of compatibility, interoperability, and integration requirements for the C3I systems.

b. Approve, document, and exercise doctrinal concepts and associated operational procedures to achieve compatibility, interoperability, and integration of C3I systems employed by U.S. military forces and, as appropriate, with coalition and allied forces.

c. Establish procedures for and ensure compliance with certification of joint interoperability of C3I systems throughout those systems' life-cycles.

4. The Heads of the DoD Components shall ensure that the provisions of section D., above, are followed during the requirements validation process, acquisition, deployment, and operation of systems and forces.

F. EFFECTIVE DATE

This Directive is effective immediately.

Donald J. Atwood Deputy Secretary of Defense

SORT: 4640.06
DOCI: DODD 4640.6
DATE: 19810626
TITL: DODD 4640.6 Communications Security Telephone Monitoring and Recording, June 26, 1981, USD(P)

Refs: (a) DoD Directive 4640.1, "Telephone Monitoring and Recording," January 15, 1980
(b) through (p), see enclosure 1

A. PURPOSE

This Directive establishes policy and procedures for the communications security (COMSEC) monitoring and recording of telephone communications.

B. APPLICABILITY

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. This Directive does not apply to signals **intelligence**; administrative telephone monitoring and recording (reference (a)); interception of oral and wire communications for law enforcement purposes (DoD Directive 5200.24 (reference (b)); technical surveillance countermeasure surveys (DoD Directive 5200.29 (reference (c)); control of compromising emanations (DoD Directive 5-5200.19 (reference (d)); management and direction of C()MSEC activities (DoD Directive C-5200.5 (reference (e)); foreign **intelligence** and counterintelligence activities (DoD 5240.1-R (reference (f)); Foreign **Intelligence** Surveillance Act of 1978 (reference (g)); and telephone monitoring during wartime or under combat conditions (DoD Directive 5230.7 (reference (h)).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

1. COMSEC telephone monitoring is a valuable asset of the U.S. Government which must be conducted in a manner that satisfies the legitimate needs of the government and protects the privacy and civil liberties of persons whose telephone communications are subject to such monitoring.

2. DoD-owned or leased telephones and telephone systems are provided for the transmission of official government communications and are subject to COMSEC telephone monitoring in accordance with this Directives the National Communications Security Directive (reference (i)) and National COMSEC Instruction 4000 (reference (j)). Use of official DoD telephones and telephone systems constitutes consent by the user to COMSEC telephone monitoring.

3. COMSEC telephone monitoring provides information not available through other sources that is essential for evaluation of DoD communications security.

4. COMSEC telephone monitoring is undertaken to:

a. Collect operational signals to measure the degree of security achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related measures;

b. Determine the information and **intelligence** value of voice communications potentially subject to interception;

c. Provide an empirical basis for improving, as effectively and efficiently as possible, the security of telephone communications against hostile interception; and

d. Assist in developing communications profiles for cover and deception measures.

5. COMSEC telephone monitoring within the Department of Defense shall be conducted only by elements of the National Security Agency/Central Security Service (NSA/CSS) and the Military Departments specifically and as designated by the Director of NSA/Chief, CSS, and the Secretaries of the Military Departments, respectively.

E. PROHIBITIONS

1. This Directive does not authorize electronic surveillance of telephone communications for law enforcement or investigative purposes, and, except as provided in this section, the information obtained from COMSEC telephone monitoring shall not be used for law enforcement or investigative purposes.

2. The sole exception to this policy is when, incidental to the COMSEC telephone monitoring authorized by this Directive, information is obtained which requires immediate action in order to prevent serious bodily harm or significant loss of property. Such information may be referred to the commander or law enforcement agency having jurisdiction over the incident. In such instances:

a. The General Counsel of the DoD Component involved shall be notified promptly.

b. COMSEC telephone monitoring of the telephone circuit concerned shall cease. No attempt to investigate further or to obtain specifically additional information of criminal activity through COMSEC telephone monitoring will occur Any subsequent electronic surveillance shall be conducted in accordance with DoD Directive 5200.24 (reference (b)) or DoD 5240.1-R (reference (f)), as appropriate.

3. This prohibition does not preclude the use of information obtained as a result of COMSEC telephone monitoring in connection with disciplinary or administrative action against DoD military or civilian personnel for knowing, willful, or negligent actions that resulted in the unauthorized disclosure of classified information.

4. COMSEC telephone monitoring or the results of COMSEC telephone monitoring shall not be used to enforce the DoD policy that limits use of DoD telephones and telephone systems to conduct of official business only. That policy shall be enforced through administrative and management techniques, such as, analysis of system-wide records, periodic briefings, and supervisory controls.

F. PROCEDURES

The procedures in this section apply to all COMSEC telephone monitoring of official DoD telephones in DoD Components.

1. Notice and Consent. Users of official DoD telephones and telephone systems shall be notified that discussion of classified information over nonsecure circuits is prohibited, official DoD telephones and telephone systems are subject to COMSEC telephone monitoring at all times, and use of such telephones and telephone systems constitutes consent to COMSEC telephone monitoring.

a. The following notice shall be displayed prominently on the cover of all official DoD telephone directories:

DO NOT DISCUSS CLASSIFIED INFORMATION ON NONSECURE TELEPHONES. OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING FOR COMMUNICATIONS SECURITY PURPOSES AT ALL TIMES.

DoD telephones are provided for the transmission of official government information only and are subject to communications security monitoring at

all times. Use of official DoD telephones constitutes consent to communications security telephone monitoring in accordance with DoD Directive 4640.6.

b. In addition to the telephone directory notice, all Heads of DoD Components shall ensure that users of official DoD telephones and telephone systems subject to COMSEC telephone monitoring receive adequate notice that their use of such telephones and telephone systems constitutes consent to COMSEC telephone monitoring. Such other forms may include, but need not be limited to, the following:

(1) Decals (DD Form 2056) attached to telephones subject to COMSEC telephone monitoring. See enclosure 3;

(2) A notification and consent form;

(3) Special memoranda from responsible senior officials;

(4) Initial briefing of new personnel and periodic rebriefings;

(5) Periodic notices in daily bulletins and similar publications; and

(6) Other means approved by the General Counsel of the DoD Component concerned.

c. The General Counsel of each DoD Component shall review the notification given to users of the Component's official DoD telephones and telephone systems subject to COMSEC telephone monitoring at least once every 2 years, and shall state in writing his or her determination of the adequacy or inadequacy of such notification to include the reasons supporting that determination. If notification is inadequate, he or she shall require implementation of those measures necessary to make notification adequate.

2. Authorization and Request

a. COMSEC telephone monitoring may be authorized only by the Secretaries of the Military Departments, the Director, NSA/Chief, CSS, and Commanders of Unified or Specified Commands, or their single designees. COMSEC telephone monitoring shall be authorized only:

(1) In DoD Components in which the Component's General Counsel has determined, pursuant to paragraph F.1.c. of this Directive, that adequate notification exists;

(2) When it will aid in protecting the national security;

(3) When it will be an effective and efficient use of COMSEC resources. This determination shall be made in consultation with the operational COMSEC elements designated pursuant to paragraph F.3.a., below; and

(4) For a reasonable period of time not to exceed 1 year.

b. Heads of DoD Components other than the Military Departments, Unified and Specified Commands, and NSA/CSS shall submit requests for COMSEC telephone monitoring to the Director, NSA/Chief, CSS, in accordance with regulations of the NSA/CSS.

c. COMSEC telephone monitoring within OSD and the Defense Telephone Service-Washington is prohibited except with the written approval of the Deputy Under Secretary of Defense for Policy, or a designee.

3. Monitoring Procedures

a. COMSEC telephone monitoring within the Department of Defense shall be conducted only by elements of NSA/CSS and the Military Departments, specifically designated respectively by the Director of NSA/CSS and the Secretaries of the Military Departments.

b. COMSEC telephone monitoring of telephone lines within the Department of Defense shall be conducted only from points within the facilities or installations of DoD Components by bridging the telephone lines at points prior to the point of association, in a main distribution frame, between official DoD telephones lines and outside lines.

c. COMSEC telephone monitoring of radio, microwave, and other free space

official telephone communications shall not be conducted, except for those official telephone communications that are transmitted over systems dedicated solely to government use and that are sent and received by transmission and reception facilities dedicated solely to government use.

4. Acquisition, Retention, and Storage Procedures. The following procedures apply to the acquisition, retention, and storage of information respecting telephone conversations acquired in the course of COMSEC telephone monitoring or produced in the course of analyzing such information.

a. COMSEC telephone monitoring shall be conducted in a manner that minimizes, to the fullest extent possible, consistent with operational requirements, the recording of communications not relevant to the COMSEC telephone monitoring mission.

b. If practical, information extraneous to the COMSEC telephone monitoring mission shall be expunged from recordings upon recognition. Any such information present on recordings, to include the identities of individual conversants, will not be transcribed or otherwise used unless required in support of actions identified in subsections E.2. and E.3.

c. All transcripts, notes, logs, and other written working materials produced in the course of COMSEC telephone monitoring or in the course of analyzing communications acquired through COMSEC telephone monitoring shall be reviewed within a reasonable period after the production of such written material to assure that information not relevant of COMSEC purposes inadvertently included has been expunged. Material retained shall be annotated to include the name of the person who conducted the review and the date of the review.

d. Except as provided below, all recordings, transcripts, notes, logs, and any other written working materials containing information acquired in connection with COMSEC telephone monitoring shall be erased or destroyed upon the issuance of a final report based upon those records or within 1 year, whichever is earlier.

e. Recordings and written working materials may be retained beyond 1 year of the issuance of a final report, only if such retention is necessary for the COMSEC mission and is first approved by officials designated by the Director, NSA Chief, CSS, for that Agency, or by the Secretaries of the Military Departments for their respective Departments.

(1) Prior to approving extended retention, the approving officials hall determine whether the material to be retained has been adequately reviewed for identification and expunction of all information not relevant to COMSEC purposes. The officials shall provide for additional review of the material, if not satisfied that adequate review has occurred.

(2) Approval of extended retention shall be in writing and shall stipulate the period of time for which the recordings or written working materials may be retained.

(3) Upon the expiration of the extended retention period, the recordings or written materials shall be erased or destroyed. No information shall be retained in any form, including recordings, written working materials, or computerized data banks, after the extended retention period has expired.

(4) This paragraph does not apply to final reports resulting from a COMSEC telephone monitoring operation.

f. Final reports or evaluations resulting from a COMSEC telephone monitoring operation:

(1) Will be retained in accordance with established record retention procedures;

(2) Shall not contain:

(a) Any information extraneous to COMSEC purposes;

(b) Accounts or summaries of particular telephone conversations monitored, except for descriptions of information that may be classified or national security-related discussed in such conversations and information necessary to understand the nature of and ways in which

classified information may have been compromised; or

(c) Sufficient data to identify individuals who participated in monitored telephone conversations.

(3) Shall have an access clause prominently displayed at the beginning of the report stating that the information in the report shall be used only for official U.S. Government COMSEC purposes.

g. To the extent consistent with E.O. 12065 and DoD 5200.1-R (references (k) and (l)), all recordings and written working material containing information acquired through COMSEC telephone monitoring shall be afforded protection at least equal to that provided material officially classified CONFIDENTIAL.

h. Except as provided in subsection F.5. of this Directive, access to any recordings, written working materials, or computerized data banks containing information acquired through COMSEC telephone monitoring shall be limited to individuals in the DoD Components designated, pursuant to F.3.a. of this Directive and assigned to COMSEC duties requiring such access. Recordings, written working materials, and computerized data banks shall be stored and maintained in a manner that will assure enforcement of these access restrictions.

5. Dissemination Procedures

a. Information respecting telephone conversations acquired through COMSEC telephone monitoring shall be disseminated outside the Department of Defense only in the following circumstances:

(1) For purposes permitted by subsections E.1. through E.3. of this Directive;

(2) Pursuant to the provisions of DoD 5200.1-R (reference (1)); and

(3) When required by a court order and approved by the General Counsel of the Department of Defense.

b. Information acquired by COMSEC telephone monitoring under this Directive shall be disseminated within or outside of the Department of Defense only as necessary for purposes of COMSEC operation and management or as provided for in subsections E.1. through E. 3. of this Directive. No information shall be disseminated within or outside of the Department or outside the operational COMSEC elements designated pursuant to paragraph F.3.a. of this Directive, unless the reviews required by paragraphs F.4.b. and c. of this Directive have been conducted.

6. Safeguarding Monitoring Equipment. Telephone monitoring and recording equipment shall be safeguarded to prevent unauthorized access.

a. To the extent consistent with operational requirements, equipment not in use shall be kept in secure and controlled storage.

b. Each element of the Military Departments and NSA/CSS authorized to conduct COMSEC telephone monitoring under paragraph F.3.a. of this Directive shall maintain records showing its inventory of COMSEC telephone monitoring equipment, the time at which each item of equipment was withdrawn from and returned to storage, the location and use of each item of equipment currently in use, and the person or persons in charge of the operation for which the equipment is being used.

c. Only those persons assigned to COMSEC duties with an element designated pursuant to paragraph F.3.a. of this Directive, shall have access to monitoring equipment in use.

7. COMSEC Telephone Monitoring Outside DoD

a. COMSEC telephone monitoring by DoD personnel of official government telephone communications outside the Department of Defense is prohibited except upon written authorization of the:

(1) Deputy Under Secretary of Defense for Policy, whenever the COMSEC telephone monitoring is to be conducted by an element of one of the Military Departments.

(2) Director, NSA/Chief, CSS, whenever the COMSEC telephone monitoring is to be conducted by that Agency.

b. Only the elements of NSA/CSS and the Military Departments specifically designated to conduct COMSEC telephone monitoring within the Department of Defense shall conduct COMSEC telephone monitoring outside the Department.

c. COMSEC telephone monitoring operations outside the Department of Defense shall be subject to restrictions respecting notice to telephone users, acquisition, retention, and dissemination of information and safeguarding of monitoring equipment equivalent to the restrictions imposed by this Directive upon such activities within the Department of Defense.

G. INFORMATION REQUIREMENTS AND RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy or designee shall review and provide overall policy guidance for the COMSEC telephone monitoring program and review and act upon requests for COMSEC telephone monitoring in accordance with paragraphs F.2.c. and F.7.a.(l) of this Directive.

2. The Director, NSA/Chief, CSS, and the Secretaries of the Military Departments shall supervise and issue directives to govern all COMSEC telephone operations and ensure that all such operations comply with this Directive. The Director and Secretaries shall each designate one official in their respective Agency or Department as the official with responsibility for oversight of COMSEC telephone monitoring to ensure compliance with the provisions of this Directive.

3. The Head of each DoD Component shall:

a. Authorize or request COMSEC telephone monitoring in accordance with the provisions of this Directive and relevant regulations of the Military Departments and NSA/CSS; and

b. Cooperate with the Director, NSA/Chief, CSS, the Secretaries of the Military Departments, the General Counsels of the DoD Components, and their designees, to ensure that the COMSEC telephone monitoring conducted within the Components is effective and complies with this Directive.

4. All records of information obtained through COMSEC telephone monitoring and associated analysis shall be maintained and disseminated in accordance with subsections F.4. and F.5. of this Directive and with the provisions of DoD Directives 5400.7 and 5400.11 (references (m) and (n)).

5. DoD Components shall report to the Deputy Under Secretary of Defense for Policy, through the General Counsels and Inspector Generals of the monitoring Component and the Component being monitored, within 5 days after discovery all telephone monitoring and recording activities conducted in violation of the provisions of this Directive.

a. These reports shall contain, at a minimum, the following items:

(1) Nature of the violation, such as, unauthorized COMSEC monitoring:

(2) Date of violation occurrence;

(3) Time of violation occurrence;

(4) Location (name of installation/activity) where the violation occurred;

(5) Individual (last name, first, M.I.) or Component responsible for the infraction;

(6) Brief summary of the incident;

(7) Corrective action taken; and

(8) Current status of the inquiry.

b. This reporting requirement has been assigned Report Control Symbol DD-POL(AR) 1564. Existing standard data elements from DoD 5000.12-N (reference are being used in this reporting requirement. Any new data elements will be registered with the Director for Management Information

Control and Analysis, Office of the Assistant Secretary of Defense (Comptroller). Data elements marked with an asterisk have been registered in the DoD Data Element Program.

c. Upon receipt of these reports, the Deputy Under Secretary of Defense for Policy and the Inspector Generals and General Counsels of the DoD Components involved shall work together to ensure that all appropriate action is taken to correct and prevent such violations.

H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to thee Deputy Under Secretary of Defense for Policy within 120 days.

FRANK C. Carlucci Deputy Secretary of Defense

Enclosures - 3 1. References 2. Definitions 3. Decal

REFERENCES, continued

(b) DoD Directive 5200.24, "Interception of Wire and Oral Communications for Law Enforcement Purposes," April 3, 1978
(c) DoD Directive 5200.29, "DoD Technical Surveillance Countermeasures (TSCN) Survey Program," February 12, 1975
(d) DoD Directive 5-5200.19, "Control of Compromising Emanations," February 10, 1968
(e) DoD Directive C-5200.5, "Communications Security (COMSEC)," April 13, 1971
(f) DoD 5240.1-R, "Procedures Governing the Activities of DoD **Intelligence** Components that Affect United States Persons," November 1979, authorized by DoD Directive 5240.1, November 30, 1979
(g) Foreign **Intelligence** Surveillance Act of 1978, Public Law No. 95-511
(h) DoD Directive 5230.7, "Wartime Information Security Program (WISP)," June 25, 1965
(i) National Communications Security Directive, June 20, 1979
(j) National COMSEC Instruction (NACSI) 4000, "Guidelines for the Conduct of Communications Security Survey Activities," January 23, 1980
(k) Executive Order 12065, "National Security Information," July 3, 1978
(l) DoD 5200.1-R, "Information Security Program Regulation," October 1980, authorized by DoD Directive 5200.1, November 29, 1978 (m) DoD Directive 5400.7, "DoD Freedom of Information Act Program," March 24, 1980
(n) DoD Directive 5400.11, "Personal Privacy and Rights of Individuals Regarding Their Personal Records," August 4, 1975
(o) DoD 5000.12-M, "DoD Manual for Standard Data Elements," June 30, 1980, authorized by DoD Instruction 5000.12, April 27, 1965
(p) DoD Directive 5160.9, "Defense Telephone Service-Washington (DTS-W)," March 22, 1973

DEFINITIONS

1. Communications Security (COMSEC). Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, emissions security, and jamming resistance) to telecommunications and to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials.

2. COMSEC Surveillance. The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation.

3. COMSEC Telephone Monitoring. Listening to, copying, or recording by any means the content of official telephone communications to provide material for analysis to determine the degree of security being provided to those communications. COMSEC telephone monitoring is one of the techniques of COMSEC surveillance.

4. Consent. The agreement by a person to permit DoD communications

security components to monitor the person's official telephone communications. Consent may be oral, written, or implied. Consent may be implied if adequate notice is provided that use of official government telephones carries with it the presumption of consent.

5. Defense Telephone Service-Washington (DTS-W). An organizational entity under the Secretary of the Army that has been assigned responsibility pursuant to DoD Directive 5160.9 (reference (p)) to provide administrative telephone communications, including AUTOVON services, to DoD elements located in the National Capital Region (NCR). The NCR includes the District of Columbia, Montgomery and Prince George's Counties in Maryland, Arlington, Fairfax, Loudoun, and Prince William Counties in Virginia, and the cities of Alexandria, Fairfax, and Falls Church in Virginia.

6. Main Distribution Frame. A distribution frame, on one part of which terminates the permanent outside lines entering the central telephone and communication facility and on the other part of which terminates the subscriber line multiple cabling. The main distribution frame is used for associating any outside line with any desired terminal in such a multiple or with any other outside lines.

7. Official DoD Telephones and Telephone Systems. Telephones or telephone systems owned or leased by the U.S. Government and used for official business purposes of the U.S. Government, including the purposes of command and control of the armed forces. Official DoD telephones do not include pay telephones, telephones that are routinely used by the press, and telephones that are located in individual or family residences and intended for private use, even when the U.S. Government owns such residences.

8. Official Telephone Communications. Telephone communications in which one or more of the parties to the communications uses an official DoD telephone.

<<|IMAGE DODD0523.gif|>>

SORT: 5010.10

DOCI: DODD 5010.10

DATE: 19720809

TITL: DODD 5010.10 **Intelligence** Career Development Program, August 9, 1972, ASD(I) thru ch 1 November 16, 1994

Refs: (a) DoD Directive 5010.10, subject as above, June 16, 1966 (hereby cancelled)
(b) DoD Directive 1430. 2, "Assignment of Responsibility for Civilian Career Programs," May 9, 1966
(c) DoD Directive 5105.25, "Defense **Intelligence** School," November 2, 1962
(d) DoD Directive 5100.47, "National Cryptologic School," April 30, 1965
(e) Presidential Memorandum, "Organization and Management of the U.S. Foreign **Intelligence** Community," November 5, 1971

I. PURPOSE

This Directive implements the applicable provisions of Presidential memorandum of November 5, 1971 (reference (e)) within the Department of Defense. It establishes policy and assigns responsibilities for the development of military and civilian **intelligence** Career Programs designed to assure the attainment of an improved DoD **intelligence** product.

IL CANCELLATION

Reference (a) is hereby superseded and cancelled.

III. APPLICABILITY

The provisions of this Directive apply to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, the Defense **Intelligence** Agency, the National Security Agency and the Central Security Service (hereinafter referred to collectively as "DoD Components").

IV. DEFINITIONS

The terms used in this Directive are defined in enclosure 1.

V. POLICY

A. The Department of Defense has a significant and recognized need for professionally competent and highly motivated **Intelligence** personnel. It is essential that all practicable measures be taken to develop and maintain viable and effective career development programs for our military and civilian **Intelligence** personnel.

B. In order to address these needs and assure the emphasis and coordination required, the Assistant Secretary of Defense (**Intelligence**), on behalf of the Secretary of Defense, and in consonance with the

provisions of DoD Directive 1430.2 (reference (b)) and this Directive, will assume overall leadership and coordinating responsibility over all DoD military and civilian career development programs in the field of **Intelligence**.

VI. OBJECTIVES

The Department of Defense is fully committed to the goal of improving the career development of all military and civilian **Intelligence** personnel, thereby improving the **Intelligence** product. The specific objectives are to:

A. Improve the DoD **Intelligence** capability, in consonance with other high priority operational and personnel requirements, through the planned development, effective motivation, and efficient use of the required numbers and types of qualified military and civilian **Intelligence** personnel.

B. Provide to all career **Intelligence** personnel opportunities for education, training, rotation, and promotion equal to their contemporaries in other career fields.

C. Insure that career **Intelligence** personnel are carefully selected, provided opportunities and incentives to increase their skills and broaden their experience, and are motivated toward primary careers in one or more areas of **Intelligence**.

D. Direct attention and emphasis toward improving the career development and advancement opportunities of civilian **Intelligence** personnel by:

1. projecting and effecting planned work assignments that follow clear lines of progression to higher skill and grade levels and to successively more responsible positions, and

2. awarding the opportunity of cross-movement and promotion to positions in and among DoD components requiring **Intelligence** professionals.

E. Augment the skills of selected career **Intelligence** personnel through varied command/managerial and/or staff assignments outside the **Intelligence** field which involve the application of **Intelligence** products and the management of resources.

F. Improve the career development programs for military General **Intelligence** and Cryptologic personnel and **Intelligence** subspecialists through the interchange of information, ideas, and successful innovations.

VII. RESPONSIBILITIES AND FUNCTIONS

A. The Assistant Secretary of Defense (**Intelligence**) is responsible to the Secretary of Defense for overseeing, guiding and coordinating all DoD component **Intelligence** career development programs for military and civilian personnel; for assuring through his personal involvement that high level interest and responsiveness are maintained by DoD components; for keeping the Secretary of Defense apprised of achievements, problems and plans; and for making recommendations with respect to **Intelligence** career development activities throughout the Department of Defense. In exercising this responsibility he will:

1. Issue DoD instructions and memoranda as necessary to further implement this Directive.

2. Assure that obstacles to fully viable "**Intelligence** career development plans and programs are identified, analyzed, and resolved in a timely manner.

3. Establish as his chief advisory body a joint "**Intelligence** Career Development Steering Group," chaired by a Deputy Assistant Secretary of Defense (**Intelligence**), and composed of senior military and civilian representatives (**Intelligence** and Personnel) from each of the Military Departments, OJCS, DIA, NSA, and OASD(M&RA). This advisory group will: identify problem areas and establish priorities, recommend plans of attack with objectives for resolving these problem areas, establish schedules for and monitor the accomplishment of these objectives, interchange information and suggestions on a timely and frank basis, and advise the Assistant Secretary of Defense (**Intelligence**) when his actions and coordination are required.

4. Review all **Intelligence** education and training programs, and insure that the Defense **Intelligence** School and the National Cryptologic School serve as the cornerstones for providing the education and training programs required in accordance with DoD Directives 5105.25 and 5100.47 (references (c) and (d)) to enhance the preparation of military and civilian **Intelligence** personnel for positions in the national and international security structure and to assist in their career development

5. Review annual status reports from the Secretaries of the Military Departments and the comments thereon by the functional directors: Director, DIA for General **Intelligence** and Director, NSA/Chief, CSS for Cryptology; and report significant accomplishments, problems, plans and recommendations to the Secretary of Defense.

6. Review the **Intelligence** organizations of DoD components to evaluate the adequacy of civilian grade structures and position opportunities to support the effective career development and advancement of civilian career **Intelligence** personnel.

7. Recommend such legislation as may be necessary to overcome impediments that may exist to the effective development and administration of **Intelligence** career development programs.

8. Coordinate with the Assistant Secretary of Defense (M&RA) in matters of **Intelligence** career development policy.

B. The Director, Defense **Intelligence** Agency will be the functional director, under the guidance and direction of the Assistant Secretary of Defense (**Intelligence**), for establishing a DoD career development program designed to provide civilian General **Intelligence** career personnel for duty with the Defense **Intelligence** Agency, Service **Intelligence** Staffs, and Unified and Specified Commands; and for reviewing and coordinating career development programs for military General **Intelligence** career personnel. In exercising this responsibility he will:

1. Act as executive agent for the development of an overall career

development program for all civilian General **Intelligence** personnel in the Department of Defense in accordance with DoD directive 1430.2 (reference (b)).

2. Delineate the civilian General **Intelligence** field within the Department of Defense and establish and maintain a referral system for all identified billets and personnel.

3. Establish in consonance with the referral system an overall assignment and promotion opportunity for civilian General **Intelligence** personnel and appropriate cross assignments for professional broadening among DoD components with General **Intelligence** elements.

4. Submit proposals, including possible required legislation to upgrade career opportunities by providing more rewarding careers for the civilian General **Intelligence** community, including the opportunity to reach higher salary levels while remaining analysts.

5. Evaluate the adequacy of career programs for military and civilian General **Intelligence** personnel by commenting on the annual status reports of the Military Departments to the Secretary of Defense and by providing appropriate comments and recommendations on the achievements, problems and plans for solving the problems within the General **Intelligence** community.

C. The Director, National Security Agency/Chief, Central Security Service will act as the functional director, in accordance with the guidance of thhat effective representatives are assigned to the **Intelligence** Career Development Steering Group and that these representatives in turn have access to the highest levels within their respective military departments for action and decision as required.

6. Evaluate the effectiveness and adequacy of career programs for military and civilian **Intelligence** personnel (including subspecialists where applicable) and commencing 1 January 1973 make comprehensive but brief annual status reports to the Secretary of Defense on achievements, problems and plans for solving the problems.

VIII. REPORTING REQUIREMENTS

The reporting requirements prescribed herein are assigned Report Control Symbol DD-I(A) 1200.

IX. EFFECTIVE DATE

The provisions of this Directive are effective immediately.

Secretary of Defense

Enclosure - 1 Definitions

5010.10 (Encl 1) Aug 9, 72

DEFINITIONS

A. Career development is the orderly growth and improvement of each individual's potential to meet organizational needs as well as personal career objectives. This is accomplished by integrating each individual's

capabilities, needs, interests and aptitudes into a planned, systematic program of education, training, and utilization that is geared to meet present and future organizational requirements.

B. Career Development Program is a formal integration of the processes of recruitment, selection, placement, job rotation, education, training, incentives and awards, and promotion to achieve the systematic development and effective utilization of skills for mission accomplishment and the orderly and equitable career progression of affected personnel.

C. **Intelligence** personnel are those DoD General **Intelligence** (including scientific and technical) personnel and Cryptologic personnel engaged in the collection, processing, analysis, production and dissemination of **Intelligence** information, or involved in the planning, programming and management of **Intelligence** resources.

D. Career **Intelligence** Personnel is a term which embraces the following:

1. Military career **Intelligence** personnel are those officers, warrant officers and enlisted personnel whose careers are being developed primarily in General **Intelligence** or Cryptology augmented, wherever possible, by varied command and/or staff assignments in other functional areas.

2. Civilian career **Intelligence** personnel are those civilians in the grades of GS-5 through GS-18 whose careers are being developed in one or more areas in the field of **Intelligence** and who are part of one of the following major divisions:

a. Civilian Cryptologic personnel are those civilian personnel who work for NSA, and those civilian Cryptologic personnel of the Central Security Service, and the Service Cryptologic Agencies.

b. Civilian General **Intelligence** personnel are those civilian Intelligencepersonnel within the Department of Defense, excluding civilian Cryptologic personnel as defined above.

3. **Intelligence** Subspecialist is a term used to identify those officers of the Military Departments whose primary specialties are other than General **Intelligence** or Cryptology but who are qualified through planned training or experience to serve in, and are periodically assigned to General **Intelligence** or Cryptology positions.

Department of Defense

DIRECTIVE

NUMBER 5025.1

July 27, 2000

Administrative Reissuance Incorporating Change 1, September 11, 2000

DA&M

SUBJECT: DoD Directives System

References: (a) DoD Directive 5025.1, subject as above, June 24, 1994 (hereby canceled)

(b) DoD Directive 5400.9 "Publication of Proposed and Adopted Regulations Affecting the Public," December 23, 1974 (hereby canceled)

(c) DoD 5025.1-M, "DoD Directives System Procedures," current edition

(d) DoD 5025.1-I "DoD Directives System Annual Index," current edition

(e) through (g), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policy and responsibilities governing DoD Directives, DoD Instructions, and DoD Publications (hereafter referred to collectively as "DoD issuances").

1.2. Cancels reference (b).

1.3. Continues to authorize the publication of references (c), (d), and (e).

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the

Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

3. DEFINITIONS

3.1. Defense Agencies and DoD Field Activities. Organizations specifically designated as Defense Agencies or DoD Field Activities under Section 191 of title 10 U.S.C (reference (f)).

3.2. Directive-type Memorandum. A memorandum issued by the Secretary or Deputy Secretary of Defense or OSD Principal Staff Assistants (PSAs) that, because of time constraints, cannot be published in the DoD Directives System at the time of signature. A DoD issuance will be issued within 180 days of signature of the memorandum.

3.3. OSD Principal Staff Assistants (PSA). OSD officials holding Presidential appointments, Assistants to the Secretary of Defense and OSD Directors or equivalents who report directly to the Secretary or Deputy Secretary of Defense.

3.4. Other Organizational Entities within the Department of Defense. Organizations established pursuant to the Secretary's authority under Sections 113 or 125 of reference (f), but excluding those designated under Section 191 of reference (d). These organizations include but are not limited to the Uniformed Services University of the Health Sciences and the National Reconnaissance Office.

3.5. Organizational Charter. A DoD Directive that establishes the responsibilities, functions, relationships, and delegated authorities, as applicable, of an OSD PSA, Defense Agency, DoD Field Activity, or other organizational entity in the Department of Defense.

4. POLICY

It is DoD policy that:

4.1. A single, streamlined, uniform system governing the preparation, coordination, approval, publication, dissemination, implementation, and internal review of DoD issuances will be maintained within the Department of Defense, in

accordance with DoD 5025.1-M (reference (c)). DoD issuances under the DoD Directives System includes the following:

4.1.1. DoD Directives that provide policy required or authorized by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by the DoD Components. Specifically, DoD Directives establish or describe policy, programs and major activities, and organizations; define missions; delegate authority; and assign responsibilities. A DoD Directive shall be approved and signed by the Secretary or Deputy Secretary of Defense.

4.1.2. DoD Instructions that implement policy, or prescribe a uniform method or delineate a specific plan of action for carrying out the policy, or provide directions or details for operating a program or activity; and assign responsibilities. A DoD Instruction implements a DoD Directive and shall be approved and signed by a PSA.
A PSA may assign program responsibilities to another PSA or the Head of a DoD Component in a DoD Instruction when the authority to do so has been delegated by a DoD Directive.

4.1.3. DoD Publications (Regulations, Manuals, and DoD issuances that are not DoD Directives or DoD Instructions) that implement or supplement DoD Directives and DoD Instructions by providing uniform procedures for management or operational systems and disseminating administrative information. A DoD Publication must be authorized by a DoD Directive or DoD Instruction and its foreword approved and signed by a PSA.

4.2. DoD Directives shall adhere to the principle of centralized policy-making with decentralized execution

by the DoD Components. As such, OSD shall focus primarily on providing policy guidance, fixing responsibility, and establishing appropriate mechanisms for feedback and oversight. The DoD Components should be provided the latitude to determine how a given policy is to be implemented at the local level. DoD Directives should be streamlined into eight pages or fewer, with no procedures.

4.3. DoD Directives shall be written in such a way to preclude requirements for the publication of implementing documents by the DoD Components. When it is necessary to establish specific parameters for action or to prescribe procedures to ensure that the guidance being promulgated is fully understood and carried out, a DoD Instruction or DoD Publication should be issued rather than requiring the DoD Components to issue separate implementing documents. When implementing documents are not required, or when the deadline for issuing implementing documents

has not been met, the DoD issuance shall be directly applicable to all elements within the DoD Component, and the Head of the DoD Component. The Head of the DoD Component shall be responsible for carrying out the DoD guidance.

4.4. Coordination

4.4.1. Mandatory Coordination. All DoD issuances must be coordinated with the General Counsel, DoD, the Inspector General, DoD, and the Director of Administration and Management.

4.4.2. Proposed DoD issuances, including changes, reissuances, and cancellations of these documents, shall be formally coordinated to solicit the views of the Heads of DoD Components as follows:

4.4.2.1. If an Assistant Secretary of Defense (ASD) is under the authority, direction, and control of an Under Secretary of Defense (USD), the USD may solicit comments from the ASD and include such comments in the USD coordination.

4.4.2.2. In the Military Departments, coordination shall be at the level of Secretary, Under Secretary, or Assistant Secretary.

4.4.3. Proposed DoD Instructions and DoD Publications, including changes, reissuances, and cancellations of these document, shall be formally coordinated to solicit the views of the Heads of DoD Components.

4.4.4. Unresolved issues in proposed Directives shall be brought to the attention of the Secretary or Deputy Secretary of Defense. Unresolved issues in proposed Instructions and Publications shall be brought to the attention of the cognizant PSA.

4.5. DoD issuances of general applicability that affect the public shall be published in the Federal Register in accordance with guidance issued by the Director of Administration and Management (reference (e)).

5. RESPONSIBILITIES

5.1. The Director of Administration and Management, Office of the Secretary of Defense, shall:

5.1.1. Serve as the DoD Regulatory Policy Officer.

5.1.2. Review, coordinate, and approve DoD issuances as rules for publishing in the Federal Register.

5.1.3. Review and coordinate on all DoD issuances.

5.1.4. Prepare organizational charters for all OSD PSAs, Defense Agencies, and DoD Field Activities, and other organizational entities within the Department of Defense.

5.1.5. Monitor compliance with section 4., above.

5.2. The Director, Washington Headquarters Service, in accordance with DoD Directive 5110.4 (reference (g)) shall:

5.2.1. Administer and operate the DoD Directives System.

5.2.2. Provide operational support and administrative services to specified DoD Components and non-DoD activities.

5.2.3. Place approved DoD issuances on the Internet.

5.2.4. Approve Administrative Instructions.

5.3. The OSD Principal Staff Assistants shall:

5.3.1. Prepare DoD issuances that are relevant and necessary to accomplish their assigned responsibilities, in accordance with DoD 5025.1-M (reference (b)).

5.3.2. Prepare, coordinate, and approve DoD Instructions within their areas of responsibility and, if authorized by their organizational charters, sign the Instructions.

5.3.3. Prepare, coordinate, and approve DoD Publications and sign the foreword.

5.3.4. Publish DoD issuances of general applicability that affect the public as rules in the Federal Register in accordance with reference (e).

5.3.5. Coordinate proposed DoD issuances with the DoD Components, as prescribed in paragraph 4.4., above, and coordinate on proposed DoD issuances originated by OSD PSAs.

5.3.6. Six months from the date of the Directive and at 5-year intervals thereafter, OSD PSAs will also:

5.3.6.1. Review all DoD issuances under their cognizance for need and currency.

5.3.6.2. Certify by memorandum to DA&M, OSD, whether the issuances will be continued, revised, or canceled. Include in the memorandum the need and currency of the issuance in accordance with reference (c).

5.3.6.3. Issue directive-type memorandums and cancel or convert them to DoD issuances, in accordance with paragraph 3.2., above.

5.4. The Heads of the DoD Components shall:

5.4.1. Review and coordinate on proposed DoD issuances relevant to their missions.

5.4.2. Issue implementing documents, when required by the OSD PSAs or considered necessary, consistent with the intent of the DoD issuances.

5.4.3. Provide copies to the appropriate OSD PSAs, in accordance with DoD 5025.1-M (reference (c)).

6. EFFECTIVE DATE

This Directive is effective immediately.

E1. ENCLOSURE 1

REFERENCES, continued

(e) Administrative Instruction No. 102, "Office of the Secretary of (OSD) Federal Register (FR) System," August 6, 1999

(f) Title 10, United States Code

(g) DoD Directive 5110.4, "Washington Headquarters Services," May 10, 1999

SORT: 5100.23

DOCI: DODD 5100.23

DATE: 19670517

TITL: DODD 5100.23 Administrative Arrangements for the **National** Security Agency, May 17, 1967, thru Ch 2, November 1, 1985

Refs: (a) DoD Directive 5-5100.20, "The **National** Security Agency"
(b) DoD Directive 5100.23, "Administrative Arrangements for the **National** Security Agency," August 25, 1959 (hereby cancelled)

I. PURPOSE

This directive Prescribes certain administrative arrangements and delegates administrative authorities required for the administration and operation of the **National** Security Agency (NSA).

II. ORGANIZATIONAL RELATIONSHIPS

The **National** Security Agency is a separately organized agency within the Department of Defense under the direction, authority and control of the Secretary of Defense who acts as executive agent of the Government for the maintenance and operation of the **National** Security Agency. To the extent applicable and consistent with the functions assigned to the Agency, Department of Defense policies, regulations, and procedures will govern the Agency's Operations. When DoD directives, instructions, or other authoritative issuances hereafter published refer to DoD components or Defense Agencies, these terms include NSA unless the issuance itself specifically exempts NSA, or the Agency had obtained an exception or modification as provided below:

A. Originators of DoD directives* instructions, and substantive changes to these documents shall ascertain and consider the views of the Director, NSA as appropriate.

B. If the Director, NSA, determines that DoD issuances would adversely affect the conduct of the mission of the Agency or interfere with its security requirements, he shall recommend to the Secretary of Defense exceptions or modifications to these issuances within 90 days from the date of their promulgation.

Ill. ADMINISTRATIVE ARRANGEMENTS

The following specific arrangements and provisions will be applied in the administration and operation of the NSA:

A. Programming, budgeting, financing, accounting, and financial reporting activities of NSA will be in conformance with policies established by the Assistant Secretary of Defense (Comptroller). Disbursing services will be provided by the military departments

B. The Director, NSA, will develop, in collaboration with the military departments, and submit to the Secretary of Defense, in accordance with applicable directives consolidated cryptologic plans and programs, together with the Director's recommendations as to requirements for military and civilian manpower, operating costs, investment in facilities and capital equipment, and research, development, test and evaluation.

C. The Director, NSA, shall make maximum use of the established facilities and services of the military departments and other DoD components wherever practicable to achieve maximum efficiency and economy.

1. The military departments and other DoD components shall provide such support to the NSA within their capabilities as may be necessary to carry out the assigned responsibilities of the Agency.

2. The need for and propriety of items procured for the NSA shall be determined by the Director, NSA, subject to DoD procurement regulations.

3. Although the Agency will operate its own printing plants, it will utilize the facilities of the military departments for the disposal of printing, binding, and related equipment that is surplus to the needs of the Agency. Such equipment will be removed promptly from the Agency facility by the military department concerned. When such equipment is being replaced, it will be removed concurrently with or prior to, as appropriate, the delivery of the replacement items. In other instances, when it is necessary for the convenience of the Agency that surplus printing equipment be removed prior to its final disposition by a military department or the General Services Administration, the cost of the removal will be borne by the Agency.

4. Other excess or surplus equipment and supplies of the Agency will be disposed of in accordance with DoD directives.

D. Statistics, reports or information which will disclose the organization or any function of the NSA, any of its activities, or the names, titles, salaries, or number of persons employed by the Agency will not be released outside the DoD to any individual, organization, or Government department or agency except when authorized by the Director, NSA, the Secretary of Defense, or other proper authority, or when required by law. Statistics and progress or status reports, including those pertaining to personnel employed by or assigned to the NSA, which are required by activities of the Office of the Secretary of Defense will be submitted by the Agency to the Directorate of Statistical Services, OASD(Comp), in accordance with the provisions of DoD Instruction 7700. 3.

E. All military and civilian positions of the NSA are hereby designated as "critical sensitive positions" and will be treated as such in connection with investigative, security clearance, and employment matters.

IV. DELEGATION OF AUTHORITY

An inclosure to this directive contains delegations of the various administrative authorities required by the Director, NSA to administer and direct the operations of the Agency.

V. EFFECTIVE DATE AND CANCELLATION

This directive is effective upon publication. Reference (b) is hereby superseded and cancelled.

Deputy Secretary of Defense

Enclosure - I Delegation of Authority

DELEGATIONS OF AUTHORITY

Pursuant to the authority vested in the Secretary of Defense, the following authorities, as required in the administration and operation of the **National** Security Agency, (NSA), are hereby delegated, subject to the authority, direction, and control of the Secretary of Defense, to the Director, NSA, or in the event of the absence or incapacity of the Director, to the person acting for him to:

1. Exercise the powers vested in the Secretary of Defense by Sections 302 and 3101 of Title 5, United States Code, and Sections 2 and 4 of Public Law 86-36, as amended (50 USC 402 note), pertaining to the establishment of positions; the fixing of basic compensation; the employment, direction, and general administration of civilian personnel of the NSA subject to the following provisions:

a. Positions established at the basic compensation equal to rates of basiccompensation authorized for Grades 16, 17 and 18 of the General Schedule (5 USC 5332) are subject to the approval of the Secretary of Defense, and

b. The rates of compensation for positions established under the provisions of Section 4 of Public Law 86-36, as amended (50 USC 402 note) will be subject to approval by the Secretary of Defense.

2. Fix rates of pay for wage board employees in relation to prevailing rates for comparable job in the locality.

3. Prescribe, as conditions of employment, that NSA employees (a) must serve any place in the world as the needs of the Agency dictate, and (b) must forego personal unofficial travel when the Director, NSA, determines that travel in the proposed area would constitue a hazard to **national** security.

4. Administer oaths of office incident to entrance into the Executive Branch of the Federal Government or any other oath required by law in connection with employment therein, in accordance with the provisions of 5 USC 2903, and to designate in writing, as may be necessary, officers and employees of the NSA to perform this function.

5. Grant additional compensation to civilian officers and employees of the **National** Security Agency who are citizens or nationals of the United States, in accordance with and not to exceed additional compensation authorized by regulations of the State Department or the Civil Service Commission, whichever is applicable, for employees whose rates of basic compensation are fixed by statute.

6. Establish advisory committees and employ or procure the services of part-time advisors as consultants and experts as approved by the Secretary of Defense for the performance of NSA functions pursuant to the provisions

of 10 USC 173, 5 USC 3109, and the agreement between the Department of Defense and the Civil Service Commission on the employment of experts and consultants dated July 22, 1959; and waive compliance with any part or all of the requirements of rules 1, 2, and 3 in paragraph V.A. of DoD Directive 5030. 13, dated April 20, 1962, for any advisory committee, other than an industry advisory committee, when the Director, NSA finds that compliance would render effective utilization of the committee impracticable and that such waiver would be in the public interest.

7. Establish an NSA Incentive Awards Board and pay cash awards to, and incur necessary expenses for the honorary recognition of (a) civilian employees of the Government whose suggestions, inventions, superior accomplishments, or other personal efforts, including special acts or services, benefit or affect NSA or its subordinate activities in accordance with the provisions of 5 USC 4501-4506 and Civil Service Commission and DoD regulations, and (b) military assignees to the Agency whose suggestions, inventions scientific achievements or other meritorious special acts or services in connection with or related to their official duties benefit or affect NSA or its subordinate activities in accordance with 10 USC 1124 and DoD Directive 5120. 15, dated 3 December 1965.

8. Authorize persona to be provisionally employed before the completion of a full field investigation provided such persons are not given access to sensitive cryptologic information while so employed, in accordance with Section 302(a) of Public Law 88-290.

In an exceptional case in which the Director makes a determination in writing that his action is necessary or advisable in the **national** interest, authorize the employment of any person, or the detail or assignment of any person to the Agency, and grant to any such person access to sensitive cryptologic information, on a temporary basic pending the completion of a full field investigation, provided in such a case priority shall be given to the full field investigation, in accordance with Section 302(a) of Public Law 88-290, DoD Directive 5210.8, dated 15 February 1962, and 5210.45, dated 9 May 1964.

9. Provide for and establish boards of appraisal to assist the Director in discharging his personnel security responsibilities to appoint the members of such boards and to make the determination that a person's employment, detail, assignment, or access to classified information is or is not in the **national** interest, in accordance with Section 302(b) of Public Law 88-290 and the provisions of Department of Defense Directive 5210.45.

10. Authorize the suspension, but not to terminate the services of an employee in the interest of **nroperty and places under the jurisdiction of the Director, NSA, pursuant to the provisions of DoD Directive 5200. 8 dated August 20, 1954.**

15. Classify, declassify and downgrade or upgrade the classification of defense information or material for which the NSA has responsibility pursuant to Executive Order 10501, dated November 5, 1953, as amended, and DoD Directive 5200.1 , dated July 8, 1957, and to designate in writing, as may be necessary, officers and employees within the NSA to perform these functions.

16. Act, with respect to NSA employees, as agent for the collection and payment of taxes imposed by Subtitle C of Title 26, United States Code,

and as such agent, to make all de terminations and certifications required or provided for under Section 3122 of Title 26, United States Code, and Section 205 (p) (1) and (2) of the Social Security Act, as amended (42 USC 405 (p) (1) and (2)).

17. Authorize and approve overtime work of NSA civilian officers and employees of NSA in accordance with the provisions of Section 550. 11 of the Civil Service Regulations.

18. Authorize and approve:

a. Travel for NSA civilian officers and employees in accordance with JointTravel Regulations, Volume 2, Department of Defense Civilian Personnel, dated July 1, 1965, as amended;

b. Temporary duty travel only for military personnel assigned or detailed to NSA in accordance with Joint Travel Regulations, Volume 1, for the Uniformed Services, dated July 1, 1965, as amended;

c. Invitational travel to persons serving without compensation whose consultive, advisory, or other highly specialized technical services are required in a capacity that is directly related to or in connection with NSA activities, pursuant to 5 USC 5703.

19. Approve the expenditure of funds available for travel by military personnel assigned or detailed to NSA for expenses incident to attendance at meetings of technical, scientific, or professional or similar organizations in such instances where the approval of the Secretary of Defense or his designee is required by law (37 USC 412).

20. Develop, establish, and maintain an active and continuing Records Management Program, pursuant to the provisions of Section 506 (b) and (c) of the Federal Records Act of 1950, as amended (44 USC 396 (b)), and when authorized, operate a records center pursuant to the provisions of 506 (c) of the Federal Records Act of 1950 (44 USC 396 (c)).

21. Enter into and administer contracts in accordance with applicable laws, DoD regulations and the Armed Services Procurement Regulations, directly or through a Military Department, a DoD contract administration services component, or other Government Department or agency, as appropriate, for supplies, equipment and services required to accomplish the mission of the NSA. To the extent that any law or executive order specifically limits the exercise of such authority to persons at the Secretarial level of a Military Department, such authority will be exercised by the Assistant Secretary of Defense (Installations and Logistics).

22. Establish and use Imprest Funds for making small purchases of material and services other than personal for NSA when it is determined more advantageous and consistent with the best interests of the Government, in accordance with the provisions of DoD instruction 7280.1, dated January 5, 1962, and the Joint Regulations of the General Services Administration - Treasury Department -- General Accounting Office, entitled "For Small Purchases Utilizing Imprest Funds.

23. Establish and maintain appropriate property accounts for NSA and--to appoint Boards of Survey, approve reports of survey, relieve personal

liability and drop accountability for NSA property maintained in the authorized Departmental Property Account which has been lost, damaged, stolen, destroyed, or otherwise rendered unserviceable, pursuant to the provisions of applicable laws and regulations.

24. Act for the Secretary of Defense before the Joint Committee on Printing, the Public Printer, and the Director, Bureau of the Budget on all matters pertaining to printing, binding, and publication requirements of the NSA.

25. Publish advertisements, notices, or proposals, in newspapers, magazines, or other public periodicals as required for the effective administration and operation of the NSA (44 USC 324).

26. Enter into support and services agreements with the military departments, other DoD components, and other Government agencies as required.

The Director, NSA, may redelegate these authorities, as appropriate, and in writing, except as otherwise specifically indicated above or as otherwise provided by law.

SORT: 5100.47

DOCI: DODD 5100.47

DATE: 19650430

TITL: DODD 5100.47 **National** Cryptologic School, April 30, 1965, ASD(SIS)

Refs: (a) DoD Directive 5-3115. 2, March 19, 1959

(b) DoD Directive 5-3115. 4, March 19, 1959

I. PURPOSE

This directive provides for the establishment of the **National** Cryptologic School as a professional educational institution of the **National** Security Agency (NSA).

II. MISSION

The **National** Cryptologic School will conduct courses of instruction related to cryptologic functions designed to:

A. Enhance the preparation of selected military officers and civilian personnel for important command, staff, and policy-making positions in the **national** and international security structure.

B. Prepare military and civilian personnel for duty in cryptologic and related activities.

C. Assist the broad career development of military and civilian personnel assigned to cryptologic functions.

III. APPLICABILITY

The provisions of this directive apply to all components of DoD.

IV. FUNCTIONS AND RESPONSIBILITIES

Under the direction of the Secretary of Defense, the Director, NSA shall:

A. Operate arid control the **National** Cryptologic School.

B. Determine the level and scope of courses of instruction to be offered by the School for both resident and non-resident use, as required for accomplishment of cryptologic missions, and establish the necessary training programs arid courses.

C. Establish for the School:

1. The total enrollment and allocation of student quotas for resident courses.

2. Criteria for selection of students for resident courses.

3. Prerequisites and regulations for participation in correspondence courses.

D. Reallocate equitably unfilled quotas for resident courses.

E. Select the Chief, **National** Cryptologic School.

V. ADMINISTRATION

A. The staff and faculty will be provided from civilian and military personnel on duty with NSA and by detail from the military departments to the school for specific training requirements.

B. Clerical support for specialized and advanced courses conducted by the School for the departments will be provided by NSA.

C. Except as provided below, NSA will be responsible for programming, budgeting, and financing of expenses incident to the **National** Cryptologic

School:

1. The pay, allowances (including subsistence) of military personnel, and the permanent change of station travel costs of military and civilian personnel assigned to the staff or faculty of the School will be borne by the DoD components from which assigned.

2. Pay, allowances and travel costs (not integral to courses of instruction) of military and civilian personnel assigned as students at the School will be borne by their respective sponsoring DoD components.

3. Equipments peculiar to cryptologic missions and required to support specialized and advanced training for the military departments will be programmed, budgeted and provided to the School by the DoD components in accordance with established DoD procedures and the related Combined Cryptologic Program.

D. The Director, NSA, shall report annually to the Secretary of Defense on the operations of the School, including recommendations as appropriate.

VI. AUTHORITY

The appropriate provisions of DoD Directives 5-3115.2 and 5-3115.4 (references (a) and (b)) apply to the Director, NSA, and his designees, in the discharge of the functions and responsibilities assigned by this directive.

VII. EFFECTIVE DATE AND IMPLEMENTATION

This directive is effective upon publication. Its provisions will be implemented as determined by the Director, NSA.

Deputy Secretary of Defense

SORT: 5100.78

DOCI: DODD 5100.78

DATE: 19860825

TITL: DODD 5100.78 United States Port Security Program, August 25, 1986, USD(P)

Refs: (a) DoD Directive C-5100.78, "United States Port Security Program,"
November 25, 1975 (hereby canceled)
(b) National Security Decision Directive Number 200, December 4, 1985

A. REISSUANCE AND PURPOSE

This Directive:

1. Updates reference (a) consistent with reference (b).

2. Outlines the authorities, responsibilities, and functions relative to appropriate security measures and programs to counter the threat posed to U.S. security interests by admitting foreign vessels into U.S. ports.

B. APPLICABILITY AND SCOPE

This Directive:

1. Applies to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joints Chiefs of Staff, the Defense **Intelligence** Agency, the Defense Investigative Service, the Defense Nuclear Agency, and the National Security Agency (hereafter referred to collectively as "DoD Components").

2. Pertains to vessels of foreign countries designated under reference (b), (hereafter called "special interest vessels"), that enter into all harbors, ports, and waterfront facilities of the United States.

C. POLICY

Foreign ship visits provide unique opportunities for multidisciplinary **intelligence** collection over a wide spectrum of collection activity, from visual observations by crewmen to complex operations such as interception of electromagnetic emanations by ship-based electronic equipment. Therefore, it is the policy of the Department of Defense to take all feasible steps to reduce the vulnerability to hostile **intelligence** collection and to prevent exploitation of the vulnerability of sensitive Defense activities in or near U.S. port areas.

D. AUTHORITIES AND RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy (DUSD/P) shall coordinate Department of Defense participation in the U.S. port security program and shall:

a. Appoint the DoD Member for Policy on the U.S. Port Security Committee.

b. As appropriate, consult with the Assistant Secretary of Defense (International Security Policy) or the Assistant Secretary of Defense (International Security Affairs) regarding international politico-military aspects of the port security program.

2. The Secretary of the Navy is designated Executive Agent for Department of Defense participation in the U.S. port security program and shall:

a. Appoint a Navy staff member to act as the DoD Member for Operations on the U.S. Port Security Committee to handle matters arising from the administration of the program in conformance to the following guidelines:

(1) Signify nonobjection to port calls in cases with no significant national security implications.

(2) Negotiate alternate dates for port calls when entry is approved subject to considerations of scheduled sensitive activity and advise the DUSD/P or designee of this.

(3) Refer to the DUSD/P requests for entry to a port that may warrant DoD objection on security grounds if denial of entry would be precedent setting for that port.

(4) After a precedent-setting denial of a port call, object to future requests, if warranted, and inform the DUSD/P or designee of this.

b. Refer congressional inquiries and all matters affecting U.S. relationships with other countries or involving policy change or interpretation to the DUSD/P.

c. Develop and apply a port security vulnerability assessment program for determining on a continuing basis the sensitivity and vulnerability of Defense and Defense-related facilities in or near port areas under the jurisdiction of the United States, including programing, budgeting, and funding.

d. Prepare and maintain lists of ports that fall into the following categories:

(1) Those considered to be vulnerable to **intelligence** collection activities against Defense and Defense-related facilities.

(2) Those not measurably sensitive from a Defense point of view and need not be, therefore, the subject of individual examination each time a special interest vessel seeks entry.

e. In collaboration with the Coast Guard arid other governmental agencies,establish such other measures as may be considered necessary to frustrate hostile **intelligence** collection efforts.

3. The Director, National Security Agency, shall designate a point of contact to assist the DoD Executive Agent in fulfilling the needs of the port security program, as required.

4. The Secretaries of the Army and the Air Force each shall designate an

appropriate organization that will have a primary responsibility to respond to the needs of the port security program, including the assignment or detail of appropriate personnel to assist the Executive Agent, as required, particularly in the conduct of the port security vulnerability assessment program.

5. DoD Components concerned shall:

a. Identify to the Executive Agent sensitive installations for which they are responsible in or near port areas to facilitate vulnerability surveys and to permit appropriate notification of special interest vessel visits.

b. Review on a continuing basis the security vulnerability of such facilities and, where feasible, institute countermeasures as needed.

c. To the extent of available resources, assist and cooperate fully with the Executive Agent for DoD participation in the U.S. port security program.

E. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Deputy Under Secretary of Defense for Policy within 120 days.

William H. Taft, IV Deputy Secretary of Defense

SORT: 5100.85

DOCI: DODD 5100.85

DATE: 19950627

TITL: DODD 5100.85 **Intelligence** Systems Board (ISB), June 27, 1995, ASD(C3I)

References: (a) Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms," March 23, 1994
(b) Title 10, United States Code
(c) Title 50, United States Code
(d) Executive Order 12333, "United States **Intelligence** Activities," December 4, 1981
(e) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** (ASD(C3I))," February 12, 1992
(f) DoD Directive 5100.35, "Military Communications-Electronics Board," May 6, 1985
(g) DoD Directive 5205.9, "Joint Military **Intelligence** Program (JMIP)," April 7, 1995

A. PURPOSE

This Directive establishes a joint ISB (hereafter referred to as "the Board") composed of representatives of the Secretary of Defense and the Director of Central **Intelligence**. The Board is to ensure the interoperability of automatic NOTE: Reference (a) uses "automatic" rather than "automated" in systems such as this. END NOTE: **intelligence** information systems is met effectively and efficiently, in a manner conducive to national security, and consistent with the authorities and duties of the Secretary of Defense and the Director of Central **Intelligence** under references (b), (c), and (d).

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

C. DEFINITIONS

1. Automatic **Intelligence** Information Systems. Electronic data processing and communications systems and facilities, and related operating standards and procedures used in or intended for use in the collection, processing, analysis, and dissemination of **intelligence**; includes automatic systems that support the exchange and dissemination of **intelligence** data through transformation, indexing, storage, retrieval, presentation, telecommunications, and teleprocessing.

2. Joint Military **Intelligence** Program (JMIP). A program for planning and budgeting Defense-wide initiatives and activities that provide **intelligence** information and support to multiple DoD customers. Included are the Defense Cryptologic Program; the Defense Imagery Program; the Defense Mapping, Charting, and Geodesy Program; and the Defense General **Intelligence** and Applications Program.

3. National Foreign **Intelligence** Program (NFIP). A planning and resources management program for which responsibility has been assigned by the President to the Director of Central **Intelligence** and having

components as defined in 50 U.S.C. 401.a. (reference (c)). Included are the program on the Central **Intelligence** Agency, the Consolidated Cryptologic Program, the General Defense **Intelligence** Program, and certain other programs within the Department of Defense. Also included are the foreign **intelligence** and counterintelligence programs of the Departments of State, Treasury, and Energy, and the Federal Bureau of Investigation.

4. Tactical **Intelligence** and Related Activities (TIARA). Those DoD **intelligence** activities planned and programmed by the sponsoring organization as required for support of the planning and conduct of tactical military operations by United States Armed Forces.

D. ORGANIZATION AND MANAGEMENT

1. The ISB

a. The Deputy Assistant Secretary of Defense (**Intelligence** and Security) (DASD(I&S)), representing the Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** (ASD(C3I)) and the Executive Director for **Intelligence** Community Affairs representing the Director of Central **Intelligence**, shall Co-Chair the Board, which shall meet on the call of either Co-Chair.

b. Members of the Board shall be senior representatives of the:

(1) Under Secretary of Defense (Comptroller).

(2) NFIP Program Managers.

(3) JMIP Program Managers.

(4) Military Service TIARA Managers.

(5) Chairman of the Joint Chiefs of Staff.

(6) Director, Defense Information Systems Agency.

(7) Director, Program Analysis and Evaluation.

(8) Community Open Source Program Office.

(9) Chairperson, Military Communications-Electronics Board.

(10) Deputy Chief of Staff for **Intelligence**; Headquarters (HQ), Department of the Army.

(11) Director of Naval **Intelligence**, Department of the Navy.

(12) Assistant Chief of Staff, **Intelligence**, HQ, Department of the Air Force.

(13) Director of **Intelligence**, HQ, U.S. Marine Corps.

c. The Co-Chairs may invite other organizations having an interest in automatic **intelligence** information systems to be represented at the Board sessions on an ex-officio basis, or to participate in the Board meetings when matters germane to their interests are addressed.

2. The **Intelligence** Systems Secretariat (ISS)

a. ISS (hereafter referred to as "the Secretariat") shall operate under the guidance of the Co-Chairs of the Board.

b. The Secretariat Director shall be appointed by the Secretary of Defense in consultation with the Director of Central **Intelligence**. The Deputy Director shall be appointed by the Director of Central **Intelligence** in consultation with the Secretary of Defense.

c. As the staff element of the Board, the Secretariat shall be staffed jointly by the Department of Defense and non-DoD **intelligence** elements.

d. The Secretariat Director may establish subcommittees, working groups, and advisory bodies, as necessary, to support activities of the Board.

e. With approval of the Board Co-Chairs, the Secretariat Director may invite U. S. Government organizations not represented on the Board to participate in specific programs or activities sponsored by the Board.

E. RESPONSIBILITIES AND FUNCTIONS

1. The Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence**, under DoD Directive 5137.1 (reference (e)), as the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for information management matters, shall represent the Secretary of Defense on Board-related matters. In the exercise of these responsibilities, the Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** shall:

a. Issue relevant DoD policy guidance, as necessary.

b. Nominate to the Secretary of Defense, in consultation with the Director of Central **Intelligence**, the Secretariat Director, and consult with the Director of Central **Intelligence** on appointment of the Secretariat Deputy Director.

c. Ensure appropriate participation by the DoD Components in activities of the Board and the Secretariat, including DoD representation in the Secretariat.

d. Ensure that the Secretariat shall operate under the guidance and direction of the Board Co-Chairs, and serves as the supporting staff element of the Board.

2. The **Intelligence** Systems Secretariat shall, in cooperation with the **intelligence** functional managers, provide administrative support to the Board, and shall conduct the day-to-day staff activities necessary to support accomplishment of the Board's responsibilities.

3. The **Intelligence** Systems Board shall:

a. Advise and make recommendations, under the guidance of its Co-Chairs, to the Secretary of Defense and the Director of Central **Intelligence** on policy and requirements on the design, development, acquisition, and operation of automatic **intelligence** information systems and architectures used by the DoD Components and by non-DoD organizations within the NFIP concerning:

(1) Enhancing interoperability of existing and planned automatic **intelligence** systems designed or intended for **intelligence** support to the U.S. Armed Forces.

(2) Integrating and enhancing interoperability among automatic **intelligence** information systems functioning within or among elements of the NFIP, JMIP, and TIARA aggregate.

(3) Improving interoperability between **intelligence** and military command and control systems.

(4) Defining interorganizational **intelligence** information architectures.

(5) Establishing an automatic **intelligence** information systems management security policy.

(6) Defining and coordinating common information handling standards and procedures.

(7) Developing program and budget guidance affecting the development and operation of automatic **intelligence** information systems.

(8) Evaluating and adopting new and improved automatic **intelligence** information management technologies.

(9) Designating a DoD or NFIP Component to serve as the Executive Agent for processes or activities of common concern.

(10) Identifying priority automatic **intelligence** information systems that require funding support for acquisition and/or operations.

(11) Designating of an Executive Agent(s) to implement and operate automatic **intelligence** systems as a service of common concern.

b. Emphasize the means to enhance the interoperability of existing and planned automatic **intelligence** information system support to operational military components.

c. In the interest of furthering interoperability of present and planned automatic **intelligence** information systems, serve as the channel for communications and other interface between the DoD Components represented on the ISB and the Military Communications-Electronics Board (MCEB) under DoD Directive 5100.35 (reference (f)). In this interface role, review and provide recommendations, as appropriate, on all communications between the ISB member Components and the MCEB that relate to automatic **intelligence** information systems and architectures.

4. The Chairperson of the Military Communications-Electronics Board shall provide a senior member to serve as a member of the ISB, and ensure that communications between the MCEB and the DoD Components represented on the ISB are sent to the ISB Secretariat for review by the ISB if they relate to automatic **intelligence** information systems and architectures.

5. The Heads of the DoD Components shall:

a. Provide senior-level representation to serve on the Board.

b. Provide qualified representatives, as coordinated with the Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** to the Secretariat on a detail, non-reimbursable, rotational basis.

c. Participate, where appropriate, in working groups and panels established by the Secretariat Director to address tasks assigned by the Board Co-Chairs.

d. Provide information and data to the Secretariat as required to enable the Board to fulfill its responsibilities.

e. Upon designation by the Secretary of Defense and Director of Central **Intelligence**, and with arrangements for necessary funding, serve as the Executive Agent for implementation and/or operation of automatic **intelligence** information systems as a service of common concern.

F. EFFECTIVE DATE

This Directive is effective immediately.

John P. White
Deputy Secretary of Defense

SORT: 5105.56

DOCI: DODD 5105.56

DATE: 19920506

TITL: DODD 5105.56 Central Imagery Office, May 6, 1992, DA&M, thru Ch1, March 19, 1993

References: (a) Title 10 of the United States Code

(b) National Security Act of 1947

(c) Executive Order 12333, "United States **Intelligence** Activities," December 4, 1981

(d) DOD Directive 5240.1, "DOD **Intelligence** Activities," April 25, 1988

(e) DOD 5240.1-R, "Procedures Governing the Activities of DOD **Intelligence** Components That Affect United States Persons," December 3, 1982.

(f) DOD Directive 7750.5, "Management and Control of Information Requirements," August 7, 1986

A. PURPOSE AND APPLICABILITY

1. This Directive establishes a Central Imagery Office (CIO) within the Department of Defense to ensure that United States Government **intelligence**, mapping, charting and geodesy, and other needs for imagery are met effectively and efficiently in a manner conducive to national security, consistent with the authorities and duties of the Secretary of Defense and the Director of Central **Intelligence** under references (a), (b), and (c).

2. This Directive applies to the Office of the Secretary of Defense, the Military Departments; the Chairman of the Joint Chiefs of Staff and the Joint Staff; the Unified and Specified Combatant Commands; the Defense Agencies; and DOD Field Activities.

B. MISSION

The CIO shall provide support to the Department of Defense, the Central **Intelligence** Agency, and other Federal Government departments and agencies on matters concerning imagery relating to the national security.

C. ORGANIZATION AND MANAGEMENT

The CIO is hereby established as a defense agency of the Department of Defense under reference (a) and is hereby designated as a combat support agency. The Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** shall exercise overall supervision over the Central Imagery Office. The CIO shall consist of a Director of the Central Imagery Office and such subordinate organizational elements, including the central imagery tasking authority required by Section E.1.d., as the Director establishes within the resources made available.

D. RESPONSIBILITIES AND FUNCTIONS

The Director of the CIO shall:

1. Organize, direct, and manage the CIO and all assigned resources;

2. Manage the establishment of national imagery collection requirements consistent with guidance received from the Director of Central **Intelligence** under reference (c);

3. Ensure responsive imagery support to the Department of Defense, the Central **Intelligence** Agency, and, as appropriate, other Federal Government departments and agencies, including by coordination of imagery collection tasking, collection, processing, exploitation, and dissemination.

4. Task imagery collection elements of the Department of Defense to meet national **intelligence** requirements, including requirements established by the Director of Central **Intelligence** in accordance with references (b) and (c), except that the Director of the CIO shall advise an imagery collection element on collection of imagery to meet such national **intelligence** requirements when the collection element both (a) is assigned to or under the operational control of the Secretary of a MilitaryDepartment or a commander of a unified or specified command and (b) is not allocated by the Secretary of Defense to meet national **intelligence** requirements.

5. Advise imagery collection elements of the Department of Defense on the collection of imagery to meet non-national **intelligence** requirements;

6. Establish, consistent to the maximum practicable extent with the overall functional architectures of the Department of Defense, the architectures for imagery tasking, collection, processing, exploitation, and dissemination within the Department of Defense, and, to the extent authorized by the heads of other departments or agencies with imagery tasking, collection, processing, exploitation, and dissemination functions establish the architectures for imagery tasking, collection, processing, exploitation, and dissemination within those departments or agencies;

7. Establish, in coordination with the Director of the Defense Information Systems Agency as appropriate, standards for imagery systems for which the Department of Defense has responsibility and ensure compatibility and interoperability for such systems, and, to the extent authorized by the heads of other departments or agencies with imagery systems establish standards and ensure compatibility and interoperabilgence Agency; and

d. establish within the CIO a central imagery tasking authority to execute the imagery collection tasking authority of the Director of the CIO.

2. The Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the heads of other Department of Defense components shall support the Director of the CIO in the performance of the Director's functions, including by:

a. ensuring compliance with national **intelligence** tasking issued under paragraph D.4 above;

b. ensuring compliance with the architectures and standards established by the Director of the CIO under paragraphs D.6, D.7, and D.15 above;

c. assisting the Director in his role as functional manager for the Consolidated Imagery Program and the Tactical Imagery Program under paragraphs D.8 and D.9 above; and

d. submitting imagery collection requirements to the Director.

F. DELEGATIONS OF AUTHORITY

1. The Assistant Secretary of Defense for Command, Control, Communications and **Intelligence** is hereby delegated the authority to issue instructions to Department of Defense components to implement this Directive. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments. Instructions to the commanders in chief of the unified and specified commands shall be issued through the Chairman of the Joint Chiefs of Staff.

2. The Director of the CIO is hereby delegated the authority to obtain reports, information, advice, and assistance, consistent with reference (f), as necessary, in the performance of the Director's assigned functions.

G. ADMINISTRATION

1. The Director of the Central Imagery Office shall be appointed by the Secretary of Defense on the recommendation of the Director of Central **Intelligence**.

2. The Director of the Central Imagery Office shall obtain administrative support, including personnel, budget execution, and contracting services, from the Defense **Intelligence** Agency and, to the extent permitted by law and approved by the Secretary of Defense and the Director of Central **Intelligence**, the Central **Intelligence** Agency.

3. Resources for the Central Imagery Office shall be provided through the National Foreign **Intelligence** Program and the budget aggregation known as Tactical **Intelligence** and Related Activities, in accordance with applicable planning, programming, and budgeting system processes.

H. EFFECTIVE DATE

This Directive shall take effect immediately.

Secretary of Defense

Department of Defense

DIRECTIVE

NUMBER 5105.67

February 19, 2002

DA&M

SUBJECT: Department of Defense Counterintelligence Field Activity (DoD CIFA)

References: (a) Title 10, United States Code

(b) Presidential Decision Directive/National Security Council-75, "U.S. Counterintelligence Effectiveness, Counterintelligence for the 21st Century," December 28, 2000

(c) Executive Order 12958, "Classified National Security Information," April 17, 1995

(d) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 13, 1997

(e) through (p), see enclosure 1

1. PURPOSE

Pursuant to the authority vested in the Secretary of Defense by reference (a), this Directive establishes the Department of Defense Counterintelligence Field Activity with the mission, responsibilities, functions, relationships, and authorities, as prescribed herein.

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities, as well as all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

3. MISSION

The mission of the DoD CIFA is to develop and manage DoD Counterintelligence (CI) programs and functions that support the protection of the Department, including CI support to protect DoD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and U.S. interests, against foreign influence and manipulation, as well as to detect and neutralize espionage against the Department.

4. POLICY

It is DoD policy that:

4.1. The Department shall fully support the National Counterintelligence Program, as embodied in Presidential Decision Directive/National Security Council-75 (PDD/NSC-75) (reference (b)), and the National Counterintelligence Executive (NCIX).

4.2. The Department will make full use of advanced technology to create and maintain a collaborative CI analytic environment to protect critical DoD and national assets.

4.3. There is a single coordination focal point for DoD CI policy implementation, Defense-wide CI resource and budget planning, and for DoD CI implementation liaison with the NCIX staff in accordance with reference (b).

4.4. All DoD CI matters and activities that affect or are related to DoD Special Access Programs (SAPs) shall comply with the security procedures of Executive Order 12958 (reference (c)), DoD Directive O-5205.7 (reference (d)), and the DoD Overprint to the National Industrial Security Program Operating Manual Supplement (reference (e)).

5. ORGANIZATION

The DoD CIFA is hereby established as a Field Activity within the Department of Defense, under the authority, direction, and control of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)). For certain functions as specified in this Directive or separately by the Secretary of Defense, the DoD CIFA shall be treated as a Combat Support Agency. It shall consist of:

5.1. A Director appointed by, and reporting to, the ASD(C3I).

5.2. The Joint Counterintelligence Evaluation Office (JCEO), the Joint CI Analysis Group (JCAG), the Defense CI Information System (DCIIS) Program Office, the Joint CI Training Academy (JCITA), and the Defense CI Force Protection Response Group (FPRG). In carrying out the mission of these elements, the Director of the DoD CIFA may employ law enforcement personnel, in whole or in part, as appropriate, to carry out the DoD CIFA's law enforcement functions as stated in paragraph 6.2.17. of this Directive.

5.3. Such additional subordinate organizational elements as are established by the Director, DoD CIFA, within authorized resources.

6. RESPONSIBILITIES AND FUNCTIONS

6.1. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), pursuant to PDD/NSC-75 (reference (a)) and in accordance with Executive Order 12333, DoD Directive 5137.1, DoD Directive 5240.2, DoD Directive 5240.1, DoD 5240.1-R, Appendix 3 of Title 5, United States Code, and DoD Directive 5200.27 (references (f), (g), (h), (i), (j), (k), and (l)), shall:

6.1.1. Exercise authority, direction, and control over the Director, DoD CIFA.

6.1.2. Serve as the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense regarding all CI policies and related matters.

6.1.3. Represent the Secretary of Defense in all matters with the NCIX.

6.1.4. Oversee the Defense CI Program.

6.2. The Director of the Department of Defense Counterintelligence Field Activity, under the authority, direction, and control of the ASD(C3I), shall:

6.2.1. Organize, direct, and manage the DoD CIFA and all assigned resources.

6.2.2. Serve as the principal advisor on DoD CI operational matters and policy-implementation activities to the OSD Principal Staff Assistants and other DoD Component officials and manage the execution of DoD CI policy issued by the ASD(C3I), pursuant to DoD Directive 5137.1 (reference (g)).

6.2.3. Develop a DoD CI implementation strategy and an implementation plan consistent with the national CI strategy, national guidance, and DoD CI strategy; the implementation plan shall include appropriate performance-measurement standards and resource metrics consistent with these aforementioned strategies.

6.2.4. Represent the Department with other Government and non-government agencies, including the NCIX staff, regarding the implementation of all DoD CI matters, and shall:

6.2.4.1. Oversee DoD implementation support to the NCIX organization.

6.2.4.2. Serve as the single coordination focal point within the Department for DoD CI program implementation, DoD CI resource planning, and DoD CI implementation liaison with the NCIX staff, to include coordination regarding NCIX decisions and functions regarding national CI resource allocations.

6.2.5. Regarding budgetary matters:

6.2.5.1. Prepare and provide, together with, and pursuant to, the policy guidance of the ASD(C3I) and submissions from the Secretaries of the Military Departments, submissions for the Department's Planning, Programming, and Budgeting System (PPBS).

6.2.5.2. Prepare and provide, together with, and pursuant to, the policy guidance of the ASD(C3I) and submissions from the Secretaries of the Military Departments, the Department's submissions to the Office of the Director of Central Intelligence for the Director of Central Intelligence Capabilities, Programming and Budgeting System (CPBS) to provide resources for the Foreign Counterintelligence Program in the National Foreign Intelligence Program, the Defense Joint Counterintelligence Program in the Joint Military Intelligence Program, and all other assigned DoD CI programs and activities.

6.2.5.3. Support the ASD(C3I)'s presentation and justification of DoD CI programs and budget throughout the PPBS process, including representations before the Congress, for all responsibilities and functions prescribed herein.

6.2.6. Develop, implement, and oversee DoD CI programs, as assigned herein, using state-of-the-art Information Technology (IT) whenever practicable, consistent with mission requirements, and consulting with the CI offices of the DoD Components to ensure the integrity of all CI IT systems.

6.2.7. Develop and manage an integrated Defense CI Program.

6.2.8. Develop and integrate the Defense CI Information System (DCIIS) Program, including, but not limited to, the architecture, software development, training, implementation,

and sustainment of the DCIIS while ensuring the architectural integrity of the system.

6.2.9. Oversee Defense-wide CI investigations, operations, and CI functional services, and:

6.2.9.1. Perform programmatic evaluations of the Department's CI activities to determine the extent to which CI policies and resources adequately protect the Department of Defense against the threats of espionage, terrorism, sabotage, assassination, and other covert or clandestine activities, including those of foreign intelligence services.

6.2.9.2. Provide appropriate and timely access to all relevant CI investigative and operational information to designated senior DoD officials with CI responsibilities.

6.2.9.3. Provide timely advice and recommendations to the ASD(C3I) and other senior DoD officials concerning potential damage to DoD or national security that could result from the compromise of classified or sensitive information. Apprise appropriate policy makers of such damage and notify them about any CI investigations that have had, or could have, a significant impact on the Department.

6.2.9.4. Facilitate the dissemination of relevant CI and CI-related information to appropriate DoD personnel who have a need-to-know.

6.2.9.5. Review and report to the ASD(C3I) any significant developments regarding both initial and on-going CI investigations and operations that affect DoD personnel and resources, with particular emphasis on those investigations and operations that have the potential to seriously compromise critical Defense technologies, the Defense Information Infrastructure, and current or near-term military operations. Such reports shall address, where appropriate, the steps that can be taken to minimize the damage caused by the associated CI threat.

6.2.9.6. Recommend DoD policies and procedures that maximize the integrity of on-going CI investigations and operations within the Department.

6.2.10. Oversee the DoD CI Research and Technology Protection (RTP) Program.

6.2.11. Conduct risk assessments in support of CI RTP, DoD Critical Infrastructure Protection, DoD Force Protection, and:

6.2.11.1. Provide course-of-action analyses, situational awareness, and tailored product support to Heads of the DoD Components and other senior officials, as appropriate.

6.2.11.2. Provide CI threat assessments and advisories, risk assessments, and multimedia dissemination to the Heads of the DoD Components.

6.2.11.3. Coordinate and integrate applicable RTP efforts with Special Access Programs, through the OSD Special Access Program Coordination Office (SAPCO).

6.2.11.4. Provide tailored analytical and data-mining support to DoD CI field elements and activities of the DoD Components, as appropriate, but, in particular, to the Directors of the Defense Intelligence Agency, the Defense Security Service, the Defense Threat Reduction Agency, and the National Security Agency, as well as the Secretaries of the Military Departments.

6.2.11.5. Work within the larger DoD Intelligence Production Program in coordination with the Director, Defense Intelligence Agency, regarding the DoD CI Production Management Program.

6.2.11.6. Conduct Domestic Threat Analyses and Risk Assessments in support of DoD Force Protection and DoD Critical Infrastructure Protection efforts.

6.2.11.7. Conduct operational analysis in support of DoD CI investigations and operations.

6.2.12. Identify and track technologies requiring protection.

6.2.13. Oversee the DoD CI Technology Horizontal Risk Assessment and JCAG Threat Mapping processes and prepare Technology and Target Profiles and Technology Risk Assessments.

6.2.14. Oversee and conduct advanced joint CI training within the Department, and:

6.2.14.1. Exercise authority, direction, and control over the DoD Joint CI Training Academy.

6.2.14.2. Develop and provide to the ASD(C3I) procedural recommendations for CI training and professional development within the Department.

6.2.15. Supervise and conduct the activities of the DoD FPRG and in activities in support of the Combatant Commanders, coordinate FPRG plans and operations with the Chairman of the Joint Chiefs of Staff (CJCS), as necessary.

6.2.16. Oversee and conduct an advanced technology development program in support of the Defense Counterintelligence Program.

6.2.17. Carry out assigned functions and responsibilities in subparagraphs 6.2.2. through 6.2.16. of this Directive with the DoD CIFA operating as a law enforcement activity within the Department of Defense pursuant to the authorities vested in the Secretary of Defense in reference (a).

Unless otherwise directed by the Secretary or Deputy Secretary of Defense, the law enforcement responsibilities assigned by this Directive do not replace or supersede those responsibilities currently assigned to the Defense Criminal Investigative Service (DCIS), the Army Criminal Investigative Division, the Naval Criminal Investigative Service, or the Air Force Office of Special Investigations as Defense Criminal Investigative Organizations (DCIOs).

Accordingly, the DoD CIFA shall not engage in the investigation, apprehension, or detention of individuals suspected or convicted of criminal offenses against the laws of the United States. For SAPs and SAP-related investigations, the DCIS or the other DCIOs dedicated to SAPs have investigative jurisdiction.

6.2.18. Handle all assigned functions and responsibilities that affect DoD SAPs or SAP-related matters through approved SAP offices, such as the OSD SAP Coordination Office or the SAP Central Offices of the Military Departments.

6.3. The Under Secretary of Defense (Acquisition, Technology, and Logistics) shall support the ASD(C3I) and the Director, DoD CIFA, in taking necessary measures to require that DoD Components with acquisition, technology, and logistics responsibilities support the implementation of CI policies, including those set forth in PDD/NSC-75 (reference (b)) and those intended to support the protection of DoD research and technology as referenced in DoD Directive 5200.39 (reference (m)) and other related Departmental issuances.

6.4. The Secretaries of the Military Departments shall:

6.4.1. Support the DoD CIFA in implementing PDD/NSC-75 (reference (b)) and integrating the Defense CI Program DoD-wide and overseeing the appropriate functional aspects

of the program.

6.4.2. Report all significant CI activities, including investigations and operations, to the Director, DoD CIFA.

6.5. The Chairman of the Joint Chiefs of Staff (CJCS) shall provide combat-support guidance to the Director, DoD CIFA, in coordination with the ASD(C3I), regarding the FPRG.

6.6. The Director, Defense Intelligence Agency, shall provide for the seamless integration of CI collection, production, and joint-operations requirements management with the activities managed and directed by the Director, DoD CIFA. The Joint Staff/J2/CI shall coordinate all joint-CI activities/requirements with the Director, DoD CIFA, and shall coordinate all DoD CIFA-related issues with the CJCS and the Combatant Commanders.

6.7. The Heads of the DoD Components shall:

6.7.1. Support the DoD CIFA on CI operational and implementation matters and shall provide for the conduct, direction, management, coordination, and control of CI activities within their respective components, pursuant to DoD Directive 5240.2 (reference (h)):

6.7.2. Report all significant CI activities regarding the respective DoD Component, including investigations and operations, to the DoD CIFA.

7. RELATIONSHIPS

7.1. In the performance of assigned duties, the Director, DoD CIFA, shall:

7.1.1. Keep the DoD Components fully informed concerning DoD CIFA activities with which they have collateral or related functions.

7.1.2. Exchange information and advice as well as coordinate actions with the DoD Components, as required, to carry out assigned responsibilities and functions.

7.1.3. Use established facilities and services in the Department of Defense and other Government Agencies, whenever practicable, to avoid duplication and achieve maximum efficiency and economy of operations.

7.1.4. Represent the Department of Defense and maintain appropriate liaison, consultation, and coordination with other governmental and non-governmental agencies and CI organizations, as required, to exchange information and advice on programs and activities in the fields of assigned responsibility.

7.2. The Heads of the DoD Components shall coordinate and consult with the Director, DoD CIFA, on matters relating to DoD CIFA operations, functions, and responsibilities.

7.3. The OSD Special Access Program Coordination Office, in coordination with the ASD(C3I) and the SAP Central Offices of the Military Departments, shall be the point of contact for all CI-related SAP issues.

8. AUTHORITIES

The Director, DoD CIFA, is specifically delegated the authority to:

8.1. Obtain reports and information consistent with DoD Directive 8910.1 (reference (n)), as necessary, to carry out assigned functions.

8.2. Communicate directly with appropriate representatives of the DoD Components, as necessary to carry out assigned functions, including the transmission of requests for advice and assistance. Communications to the Military Departments shall be transmitted through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary of Defense in other DoD issuances. Communications to the Commanders of the Combatant Commands shall be transmitted by the ASD(C3I) through the CJCS.

8.3. Communicate with other Government officials, representatives of the legislative branch, members of the public, and representatives of foreign governments, as appropriate, in carrying out assigned functions.

8.4. This Directive does not supersede any of the provisions of DoD Directive O-5205.7 or DoD Overprint to the NISPOMSUP (references (d) and (e)).

8.5. Exercise the administrative authorities in enclosure 2.

9. ADMINISTRATION

9.1. The Secretaries of the Military Departments shall assign military personnel to the DoD CIFA in accordance with approved authorizations and established procedures for assignment to joint duty.

9.2. Administrative support for the DoD CIFA shall be provided by appropriate DoD Components through inter-Service support agreements in accordance with DoD Instruction 4000.19 and DoD Directive 1400.16 (references (o) and (p)).

10. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 2

E1. References, continued

E2. Delegations of Authority

E1. ENCLOSURE 1

REFERENCES, continued

(e) Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement, January 14, 1998

(f) Executive Order 12333, "United States Intelligence Activities," December 4, 1981

(g) DoD Directive 5137.1, "Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I))," February 12, 1992

(h) DoD Directive 5240.2, "DoD Counterintelligence," May 22, 1997

(i) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988

(j) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982

(k) Appendix 3 of title 5, United States Code, "Inspector General Act of 1978," as amended

(l) DoD Directive 5200.27, "Acquisition of Information

Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980

(m) DoD Directive 5200.39, "Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection," September 10, 1997

(n) DoD Directive 8910.1, "Management and Control of Information Requirements," June 11, 1993

(o) DoD Instruction 4000.19, "Interservice and Intragovernmental Support," August 9, 1995

(p) DoD Directive 1400.16, "Inter-departmental Civilian Personnel Administration Support," October 30, 1970

E2. ENCLOSURE 2

DELEGATIONS OF AUTHORITY

E2.1.1. Pursuant to the authority vested in the Secretary of Defense, and subject to the authority, direction, and control of the Secretary of Defense, the ASD(C3I), and in accordance with DoD policies, Directives, and Instructions, the Director, DoD CIFA, or in the absence of the Director, the person acting for the Director, is delegated authority, as required, in the administration and operation of the DoD CIFA to:

E2.1.1.1. Perform the following functions in accordance with Executive Order 10450, Executive Order 12333, Executive Order 12968, and DoD Directive 5200.2, as appropriate, to:

E2.1.1.1.1. Designate any position in DoD CIFA as a "sensitive" position.

E2.1.1.1.2. Authorize, in case of emergency, the appointment of a person to a sensitive position in the DoD CIFA for a limited period of time and for whom a full field investigation or other appropriate investigation, including National Agency Check, has not been completed.

E2.1.1.1.3. Authorize the suspension, but not terminate the services of, a DoD CIFA employee in the interest of national security.

E2.1.1.2. Authorize and approve:

E2.1.1.2.1. Temporary duty travel for military personnel assigned or detailed to the DoD CIFA in accordance with Joint Federal Travel Regulations, Volume 1.

E2.1.1.2.2. Travel for DoD CIFA civilian employees in accordance with Joint Travel Regulations, Volume 2.

E2.1.1.2.3. Invitational travel to non-DoD employees whose consultative, advisory, or other highly specialized technical service are required in a capacity that is directly related to, or in connection with, DoD CIFA activities, in accordance with Volume 2, Joint Travel Regulations.

E2.1.1.2.4. Overtime work for DoD CIFA civilian employees in accordance with 5 U.S.C. Chapter 55, Subpart V, and applicable Office of Personnel Management (OPM) regulations.

E2.1.1.2.5. Approve the expenditure of funds available for travel by military personnel assigned or detailed to the DoD CIFA for expenses incident to attendance at meetings of technical, scientific, professional, or other similar organizations in such instances where the approval of the Secretary of Defense, or designee, is required by 37 U.S.C. 412, and 5 U.S.C. 4110 and

4111.

E2.1.1.2.6. Develop, establish, and maintain an active and continuing Records Management Program, pursuant to 44 U.S.C. 3102 and DoD Directive 5015.2.

E.2.1.1.2.7. Authorize the publication of advertisements, notices, proposals, or other public periodicals, as required for the effective administration of DoD CIFA, consistent with 33 U.S.C. 3702.

E2.1.1.2.8. Establish and maintain, for the functions assigned, an appropriate publications system for the promulgation of Directives, Instructions, Publications, and reference documents, and changes thereto, pursuant to the policies and procedures prescribed in DoD 5025.1-M.

E2.1.1.2.9. Enter into support and services agreements with the Military Departments, other DoD Components, or other Government Agencies, as required, for the effective and efficient performance of DoD CIFA responsibilities and functions.

E2.1.1.2.10. Enter into and administer contracts directly or through a Military Department, a DoD contract administration services component, or other Government Department or Agency, as appropriate, for supplies, equipment, and services required to accomplish the mission of DoD CIFA.
To the extent that any law or Executive order specifically limits the exercise of such authority to persons at the Secretarial level of a Military Department, such authority will be exercised by the appropriate Under Secretary or Assistant Secretary of Defense.

E2.1.1.3. The Director, DoD CIFA, may redelegate these authorities, as appropriate and in writing, except as otherwise specifically indicated above or as otherwise provided by law or regulation.

SORT: **5200**.12
DOCI: **DODD 5200**.12
DATE: 19920727
TITL: **DODD 5200**.12 Conduct of Classified Meetings, July 27, 1992, ASD(C3I)

Refs: (a) DoD Directive **5200**.12, "Conduct of Classified Meetings," May 16, 1988 (hereby canceled)
(b) DoD **5200**.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive **5200**.1, June 7, 1982
(c) DoD 5220.22-R, "Industrial Security Regulation," December 1985, authorized by DoD Directive 5220.22, December 8, 1980
(d) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified information, January 1991, authorized by DoD Directive 5220.22, December 8, 1980
(e) through (j), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update DoD policy, procedures, and responsibilities for the conduct of classified meetings.

B. APPLICABILITY AND SCOPE

1. This Directive:

a. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components")

b. Applies to those classified meetings defined in enclosure 2.

2. Does not apply to in-house gatherings, to routine gatherings of U.S. Government officials, to classes conducted by DoD schools, or to gatherings between personnel of a DoD Component and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific government contract, program or project, such as program reviews. Security for such gathering s must be commensurate with the requirements of references (b),(c), and (d) to protect and control access to classified information presented at the gatherings.

C. DEFINITIONS

The terms used in this Directive are defined in enclosure 2.

D. POLICY

The dissemination of classified information to large audiences increases security risks and may involve substantial costs to provide adequate security. Therefore, DoD policy is as follows:

1. The number of meetings involving dissemination of classified information must be limited and those conducted shall be authorized only when the Head of the appropriate DoD Component, or a designee, determines the following in writing:

a. Conduct of the classified meeting serves a specific U.S. Government purpose.

b. The use of other prescribed channels for dissemination of classified information does not accomplish the purpose.

c. The location selected for the meeting is under the security control of a U.S. Government Agency or a U.S. contractor having an appropriate facility security clearance.

d. Adequate security procedures have been developed and can be implemented.

2. The conduct of a classified meeting shall be authorized by the Head of a DoD Component that has a principal interest in the subject matter of the meeting. This responsibility may be delegated. However, if the meeting involves a non-Government organization or foreign participation, it shall be delegated only as follows:

a. To a person serving in a position at or above the level of deputy assistant secretary or equivalent for the OSD.

b. The senior security official in the Military Departments. (See DoD **5200**.1-R, subsection 13-301 (reference (b)).)

c. The Director of the Joint Staff.

d. The Directors of Defense Agencies.

(Written authorization by the appropriate DoD official shall be obtained following the procedures described in section F., below, before any commitments are made or any announcements are published on the conduct of a classified meeting.)

3. The Heads of the DoD Components, or their designees, following the procedures described in section F., below, may authorize organization of and administrative support to classified meetings by non-Government organizations. However, the authorizing official shall retain full responsibility for all security aspects of the classified meeting. This responsibility shall include decisions on what classified information is to be presented, the level of classification to be assigned to the meeting, and the propriety of permitting attendance by foreign nationals.

4. Classified presentations shall be segregated from unclassified presentations to the maximum extent practicable.

a. Classified sessions shall be held ONLY at a U.S. Government installation or a U.S. contractor facility where adequate physical security and procedural controls have been approved.

b. Post or base theaters and other facilities normally open to uncontrolled access may be used for classified meetings only if no secure facility is available and unauthorized physical and aural access is prevented during the course of the meetings. A technical surveillance countermeasures (TSCM) survey may be conducted if deemed necessary by the TSCM program manager of one of the DoD Components listed in DoD Instruction 5240.5, paragraph E.l.f. (reference (e)), after consideration of relevant factors, such as sensitivity of the information to be presented, proximity to foreign embassies or consulates, and the degree of day-to-day public access to the post, base, or facility. The TSCM program manager should base his or her decision on the probability of installation of technical monitoring equipment by a hostile intelligence service at the facility to be used for the meeting.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence:

a. Shall be responsible for the effective implementation of this Directivewithin the Department of Defense.

b. May make exceptions to the requirements of this Directive on a case-by-case basis when he or she determines that doing so furthers the mission of the Department of Defense and is consistent with the protection of classified information from unauthorized disclosure.

2. The Heads of the DoD Components shall establish procedures to ensure compliance with this Directive.

F. PROCEDURES

1. The initial steps in the process of organizing a classified meeting, subject to this Directive, are to certify the Government's purpose for conducting the meeting, establish conditions under which the meeting shall be organized, and obtain the required authorization. The authorization foreach meeting shall establish that the policy requirements in subsection D.l., above, are satisfied, and describe, as a minimum, the following:

a. The subject of the meeting and scope of classified topics, to include the maximum authorized classification level.

b. The expected dates and location of the meeting.

c. The degree to which foreign participation shall be permitted, if appropriate, either by nationality, personal identity, organization affiliation, or a combination thereof. (See DoD Instruction 5230.20, paragraph E.l.d. (reference (f)).

d. The general content of the proposed announcement and/or invitation to be sent to prospective attendees or participants.

e. The identity of any non-Government organization involved, and a full description of the type of support it shall provide.

f. The security arrangements necessary to comply with DoD **5200**.1-R DoD 5220.22-R, and DoD 5220.22-M (references (b), (c), and

2. The DoD official who authorizes the classified meeting shall appoint a security manager for the meeting. The security manager shall be a DoD official of sufficient rank and experience to ensure that the requirements of this Directive; references (b), (c), and (d); and DoD Instruction 5230.20 (reference (f)) are met. The DoD security manager may use the services of a U.S. contractor that holds an appropriate facility security clearance or a U.S. Government organization to assist with implementation of security requirements under the DoD security manager's supervision.

3. The location selected for the classified sessions of the meeting must provide for proper control of access and dissemination of the classified information to be presented, and must have a secure storage capability, if necessary.

4. The content of announcements and invitations concerning classified meetings shall be approved by the DoD security manager before dissemination.

a. Announcements of classified meetings shall be unclassified and shall belimited to a general description of topics expected to be presented, names of Speakers and administrative instructions for requesting invitations or participation. They shall not describe the specific classified subjects that are to be presented or solicit classified presentations until the requirements-of subsection F.l., above, have been satisfied. The announcements then only may state that a DoD Component has authorized the conduct of classified sessions and provide instructions on application for attendance and security requirements. In this case, the announcement shallfurther specify that security clearances and justification for attendance are to be forwarded to the DoD security manager, or his or her specified designee.

b. Foreign governments shall be invited, as appropriate, after the DoD security manager determines that the applicable requirements of this Directive and DoD Instruction 5230.20 (reference (f)) shall be satisfied. Invitations to foreign governments shall be sent by the DoD Component conducting the meeting to the applicable foreign embassy in the United States or to the applicable U.S. embassy abroad. The invitation shall require that each invited foreign government provide identification of its representatives and security assurances in compliance with visit request procedures described in reference (f).

5. Access to classified meetings shall be authorized only to those persons whose security clearance and requirement for attendance have been certified by the security officer of the organization represented. The names of all properly authorized attendees or participants must appear on an access list with entry permitted to the classified meeting only after verification by the DoD security manager, or his or her designee, based on presentation of official photographic identification (e.g., passport, contractor identification card, etc.).

6. Classified information to be presented must be authorized for disclosure in advance by the U.S. Government Department or Agency having classification jurisdiction over the information involved. If there is to be participation by foreign nations, each U.S. Government and U.S. contractor employee also must provide a written assurance by the

responsible U.S. Government foreign disclosure office that their presentation has been cleared for foreign disclosure in compliance with DoD Directive 5230.11 (reference (g)). This requirement may be satisfied for U.S. contractors by a valid export license. In the absence of such assurances, the classified presentation shall not be permitted.

7. Classified presentations shall be delivered orally and/or visually. Classified documents shall not be distributed and classified note-taking and electronic recordings shall not be permitted by attendees during classified presentations. However, a DoD Component that conducts a classified meeting may compile and distribute classified presentations to authorized representatives of Government Agencies and cleared U.S. contractors having storage capability subject to compliance with DoD **5200**.1-R (reference (b)). A DoD Component similarly may authorize compilation and distribution of classified presentations on its behalf. The release of classified presentations to foreign governments and their representatives shall be in compliance with DoD Instruction 5230.20 (reference (f)) and DoD Directive 5230.11 (reference (g)).

8. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence shall be provided a copy of all authorizations for classified meetings that are conducted in collaboration with a non-Government organization or association; the information specified in subsection F.l., above, shall be included. The Director, National SecurityAgency/Chief, Central Security Service, shall be notified in the case of participation by foreign representatives in meetings involving special intelligence in accordance with DoD Directive C-5230.23 (reference (h)).

9. Reports of knowing, willful, or negligent disclosures of classified information at classified meetings to unauthorized persons shall be forwarded to the Director, Counterintelligence, Office of the Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures), Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

G. INFORMATION REQUIREMENTS

The information requirements of this Directive are exempt from licensing by paragraphs E.4.g. and E.4.h. of DoD 7750.5-M (reference (i)).

H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence within 120 days.

Donald J. Atwood Deputy Secretary of Defense

Enclosures - 2 1. References 2. Definitions

REFERENCES, continued

(e) DoD Instruction 5240.5, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," May 23, 1984
(f) DoD Instruction 5230.20, "Visits and Assignments of Foreign Representatives," April 24, 1992
(g) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984
(h) DoD Directive C-5230.23, "Intelligence Disclosure Policy (U)," November 18, 1983
(i) DoD 7750.5-M, "Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 7750.5, August 7, 1986
(j) Executive Order 12356, "National Security Information," April 16, 1982

DEFINITIONS

1. Announcement. General notification of a proposed meeting that is distributed to the public or to the membership of an organization or association.

2. Classified Information. Information or material that is:

a. Owned by, produced for or by, or under the control of the U.S. Government.

b. Determined by E.0. 12356 (reference (j)) or prior orders to require protection against unauthorized disclosure.

c. So designated.

3. Classified Meeting. A conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disseminated, but exclusive of gatherings exempted, under subsection B.2. of this Directive.

4. Foreign National. A person who is not a citizen or national of the United States.

5. In-house Meeting. A gathering of DoD personnel assigned to the same DoDComponent or of employees of the same DoD contractor.

6. Invitation. A formal request or solicitation to participate in or attend a meeting that is sent directly to a person or group of persons.

7. Security Manager. A DoD official designated to be responsible for supervising all security aspects of a classified meeting.

Department of Defense

DIRECTIVE

NUMBER 5200.28

March 21, 1988

USD(A)

SUBJECT: Security Requirements for Automated Information Systems (AISs)

References: (a) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972 (hereby canceled)

(b) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982

(c) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," October 6, 1981

(d) DoD Directive S-5200.19, "Control of Compromising Emanations (U)," February 10, 1968

(e) through (v), see enclosure E1.

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues and revises reference (a) to update uniform policy in addition to the policy set forth in reference (b) for the safeguarding of classified, sensitive unclassified, and unclassified information processed in AISs.

1.2. Updates the DoD-wide program for Automated Information System (AIS) security.

1.3. Provides mandatory, minimum AIS security requirements. More stringent requirements may be necessary for selected systems based on an assessment of acceptable levels of risk.

1.4. Promotes the use of cost-effective, computer-based (e.g., hardware, software, and firmware controls) security features for AISs. However, it is emphasized that system users have a personal responsibility to protect classified information under subparagraph 10-101.a. of reference (b).

1.5. Requires a more accurate specification of overall DoD security requirements for AISs that process classified or sensitive unclassified information.

1.6. Stresses the importance of a life-cycle management approach to implementing computer security requirements.

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments and the Military Services within those Departments, the Joint Chiefs of Staff (JCS), the Joint Staff, the Unified and Specified Commands, the Defense Agencies, the DoD Field Activities, and such other offices, Agencies, activities, and commands as may be established or designated by law, by the President, or by the Secretary of Defense (hereafter referred to collectively as "DoD Components").

2.2. This Directive applies to the following classes of information:

2.2.1. Classified information. Thereby, supplementing DoD 5200.1-R (reference (b)) for such information when contained in the AISs.

2.2.2. Sensitive unclassified information.

2.2.3. Unclassified information.

2.3. This Directive applies to all AISs including stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; embedded computer systems; communications switching computers; personal computers; intelligent terminals; word processors; office automation systems; application and operating system software; firmware; and other AIS technologies, as may be developed.

2.4. This Directive, reference (b), and DoD Directive C-5200.5 (reference (c)) apply to transmission and communications media connecting components of or to an AIS.

2.5. This Directive, DoD Directive S-5200.19 (reference (d)), NACSI 5004 (reference (e)), and NACSI 5005 (reference (f)) apply to the emanations security requirements of AISs.

2.6. This Directive and DCID No. 1/16 (reference (g)) apply to AISs processing foreign intelligence and/or counterintelligence information.

2.7. This Directive and SM-313-83 (reference (h)) apply to AISs processing Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).

2.8. This Directive and DoD Instruction 5215.2 (reference (i)) apply to the reporting and dissemination of AIS technical vulnerabilities and corrective measures.

2.9. All AISs that handle classified, sensitive unclassified, or unclassified information shall comply with the pertinent requirements of this Directive. Unless otherwise required by the Designated Approving Authority (DAA), AISs that meet any of the following conditions shall be excluded from meeting policy subsections 4.5. through 4.7., below, of this Directive:

2.9.1. AISs that are operated only in the dedicated security mode.

2.9.2. Personal computers, word processors, and similar stand-alone AISs in which it technically is not feasible to configure the equipment to support internal security controls. Such AISs may be characterized as being single-state machines without a privileged instruction set or memory lock features, and shall be operated only in the dedicated mode.

2.9.3. An AIS that is embedded in a larger system and is not removed easily, is without users, and normally receives input from, or gives output only to, other parts of the system.

2.10. AIS networks must be examined on a case-by-case basis for application of policy in this Directive. The DAA for the network should obtain guidance through established command channels, from the National Security Agency. (NSA), or where applicable, from the Defense Intelligence Agency (DIA) on evaluation and accreditation (see enclosure E5.).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure E2.

4. POLICY

It is DoD policy that:

4.1. Classified information and sensitive unclassified information shall be safeguarded at all times while in AISs. Safeguards shall be applied so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required. When classified information is involved, the information security requirements in DoD 5200.1-R (reference (b)) shall be met.

4.2. Unclassified information while in AISs shall be safeguarded against tampering, loss, and destruction and shall be available when needed. This is necessary to protect the DoD investment in obtaining and using information and to prevent fraud, waste, and abuse. Suggested safeguards for unclassified information are in OMB Circular No. A-130 (reference (j)), and include applicable personnel, physical, administrative, and technical controls.

4.3. The safeguarding of information and AIS resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications security, emanations security, and computer security (i.e., hardware, firmware, and software), as required. The mix of safeguards selected shall achieve the requisite level of security or protection.

4.4. The mix of safeguards selected for an AIS that processes classified or sensitive unclassified information shall ensure the AIS meets the minimum requirements as set forth in enclosure E3. These minimum requirements shall be met through automated and manual means in a cost-effective and integrated manner. An analysis shall be performed using enclosure E4. to identify any additional requirements over and above the set of minimum requirements.

4.5. Computer security features of commercially produced products and Government-developed or -derived products shall be evaluated (as requested) for designation as trusted computer products for inclusion on the Evaluated Products List (EPL). Evaluated products shall be designated as meeting security criteria maintained by the National Computer Security Center (NCSC) at NSA defined by the security division, class, and feature (e.g., B, B1, access control) described in DoD 5200.28-STD (reference (k)).

4.6. The following timetable shall be adhered to:

4.6.1. All AISs that process or handle classified and/or sensitive unclassified information and that require at least controlled access protection (i.e., class C2

security), based on the risk assessment procedure described in enclosure E4., shall implement required security features by 1992.

4.6.2. If security features above class C2 are required for an AIS, based on the risk assessment procedure described in enclosure E4., a timetable for meeting these more stringent requirements shall be determined on an individual system basis and submitted to the DAA for approval.
These requirements shall be met either by implementing trusted computer products listed on the EPL or by using a product not on the EPL that has security features that meet the level of trust required for the AIS.
In either case, to assess whether adequate security measures have been taken to permit the AIS to be used operationally, an accreditation must be accomplished and approved by the cognizant DAA.

4.7. There are cases where introduction of additional computer-based security features, according to the schedule given in subsection 4.6., above, for an existing AIS or an AIS already under development, may be prohibitively expensive, time-consuming, unsound technically, or adversely may impact operational effectiveness to an unacceptable degree. In such cases, the following shall apply:

4.7.1. Other safeguards (e.g., physical controls, administrative controls, etc.) may be substituted as long as the requisite level of system security or protection, as determined by the DAA, is attained.

4.7.2. Exceptions to subsection 4.6., above, may be authorized only by the DoD Component Head, or a senior DAA appointed by the DoD Component Head. Such authorization shall be based on a written determination that one or more of the conditions of subsection 4.7., above, exists.
Exceptions shall be reviewed at each reaccreditation.

4.8. When AISs managed by different DAAs are interfaced or networked, a memorandum of agreement (MOA) is required that addresses the accreditation requirements for each AIS involved. The MOA should include description and classification of the data; clearance levels of the users; designation of the DAA who shall resolve conflicts among the DAAs; and safeguards to be implemented before interfacing the AISs. MOAs are required when one DoD Component's AIS interfaces with another AIS within the same DoD Component or in another DoD Component and when a contractor's AIS interfaces with a DoD Component's AIS or to another contractor's AIS.

4.8.1. For a multi-user telecommunications network (e.g., the Defense Data Network or the World Wide Military Command and Control System Intercomputer Network), a DAA shall be designated as responsible for the overall security of the network and shall determine the security and protection requirements for connection of AISs to the network.

4.8.2. Necessary safeguards shall be agreed to and implemented and the AISs accredited for interconnection before they are connected to the network.

4.8.3. The security of each AIS connected to the network remains the responsibility of its DAA.

4.8.4. The DAA responsible for the overall security of the network shall have the authority and responsibility to remove from the network any AIS not adhering to the security requirements of the network.

4.8.5. It is permissible to define network interfaces and boundaries into manageable subnetworks based upon physical or logical boundaries, when there is a need to do so. Cryptographic separation and/or equivalent

computer security measures, as defined by the NSA or the DIA where applicable, shall be a basis for defining such network and/or subnetwork interfaces or boundaries.

4.8.6. Networks, including all connected subnetworks, shall be accredited for the highest division and class of security required based on the concepts and procedures in enclosures E4. and E5.

4.9. Security policy shall be considered throughout the life cycle of an AIS from the beginning of concept development, through design, development, operation, and maintenance until replacement or disposal. A DAA shall be designated as responsible for the overall security of the AIS. The following conditions shall be met:

4.9.1. The AIS developer is responsible for ensuring the early and continuous involvement of the users, information system security officers, data owners, and DAA(s) in defining and implementing security requirements of the AIS. There shall be an evaluation plan for the AIS showing progress towards meeting full compliance with stated security requirements through the use of necessary computer security safeguards.

4.9.2. Mandatory statements of safeguard requirements shall be included, as applicable in the acquisition and procurement specifications for AISs. The statements shall be the result of an initial risk assessment, and shall specify the level of trust required under DoD 5200.28-STD (reference (k)).

4.9.3. No classified or sensitive unclassified data shall be introduced into an AIS without designation of the classification and sensitivity of the data. Approval to enter the data shall be obtained from the data owner where applicable.

4.9.4. The accreditation of an AIS shall be supported by a certification plan, a risk analysis of the AIS in its operational environment, an evaluation of the security safeguards, and a certification report, all approved by the DAA. Accreditation of computers embedded in a system may be at the system level.

4.9.5. A program for conducting periodic reviews of the adequacy of the safeguards for operational, accredited AISs shall be established. To the extent possible, reviews are to be conducted by persons who are independent of the user organization and of the AIS operation or facility.

4.9.6. Where required, as specified in OMB Circular No. A-130 (reference (j)), a program for developing and testing contingency plans shall be established. The objective of contingency planning is to provide reasonable continuity of AIS support if events occur that prevent normal operations. The plans should be tested periodically under realistic operational conditions.

4.9.7. Changes affecting the security of an AIS must be anticipated. Any changes to the AIS or associated environment that affect the accredited safeguards or result in changes to the prescribed security requirements shall require reaccreditation. Reaccreditation shall take place before the revised system is declared operational. Minimally, an AIS shall be reaccredited every 3 years, regardless of changes.

4.10. Access by foreign nationals to a U.S. Government-owned or U.S. Government-managed AIS may be authorized only by the DoD Component Head, and shall be consistent with the Department of Defense, the Department of State (DoS), and the Director of Central Intelligence (DCI) policies.

4.11. An AIS accredited to process and/or store Sensitive Compartmented Information (SCI) may use automated means (software, firmware, or hardware) to permit classified non-SCI data to be extracted from the SCI system for use at the non-SCI classified level. This capability is permissible only if it was considered and approved as part of the security accreditation and the AIS is operating at a minimum security class of B1.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) shall:

5.1.1. Oversee and review implementation of this Directive.

5.1.2. Develop overall AIS security policies and procedures in accordance with U.S. national policies and Directives in coordination with the Under Secretary of Defense (Policy) (USD(P)), and consistent with DoD policies under DoD 5200.1-R (reference (b)), DoD Directive 7920.1 (reference (l)), DCID No. 1/16 (reference (g)), and DoD Instruction 5210.74 (reference (m)).

5.1.3. Promulgate Instructions, Standards, Manuals, and other issuances, as required, in accordance with this Directive.

5.1.4. Represent the Department of Defense on interagency committees engaged in development of security policy, standards, and criteria for AISs.

5.2. The Deputy Under Secretary of Defense (Policy) (DUSD(P)) shall continue to review, oversee, and formulate overall policies that govern DoD security practices and programs, to include developing, coordinating, and presenting DoD positions on the following:

5.2.1. Information Security.

5.2.2. Physical Security.

5.2.3. Personnel Security.

5.2.4. Industrial Security.

5.3. The Director, Defense Investigative Service (DIS), shall implement an AIS security program for DoD contractor AISs in accordance with DoD Directive 5220.22 (reference (n)) and DoD 5220.22-R (reference (o)).

5.4. The Director, Defense Communications Agency (DCA), shall implement an AIS security program for long-haul communication systems that do not handle SCI and shall certify devices that perform secured or protected telecommunications switching functions.

5.5. The Director, Defense Intelligence Agency (DIA), shall implement a program for the security of DoD Component and DoD contractor AISs and networks (e.g., the DoD Intelligence Information System network) that handle SCI. The program shall not apply to AISs and networks under the cognizance of the National Security Agency and/or the Central Security Service (NSA/CSS).

5.6. The National Security Agency and/or the Central Security Service (NSA/CSS) shall:

5.6.1. Implement an AIS security program for all AISs under NSA/CSS jurisdiction, including those of NSA/CSS contractors.

5.6.2. As requested, provide DoD Components with communications and computer security assistance and advice in support of effective AIS security measures.

5.6.3. Establish and maintain technical standards and criteria for evaluating and certifying trusted computer products. Review, at least yearly, DoD 5200.28-STD (reference (k)) and provide recommendations for revision to the ASD(C3I).

5.6.4. Provide training for DoD Components in evaluation techniques and procedures as applicable to reference (k), and certify such DoD Components to conduct evaluations.

5.6.5. Evaluate computer products intended for use by DoD Components or contractors as trusted computer products. These evaluations may be conducted on computer products developed or derived by either industry or Government sources. Also, perform quality assurance and certify evaluations performed by DoD Components.

5.6.6. Maintain and publish the EPL of evaluated industry and Government-developed or -derived trusted computer products.

5.6.7. Conduct, approve, and sponsor research and development of techniques and equipment for trusted computer products and for computer security evaluation and verification methods and techniques.

5.6.8. Serve as the focal point for technical matters on using trusted computer products and systems and, with DoD Component computer security testing and evaluation activities, provide technical advice to the DoD Components on using trusted products and systems.

5.6.9. Ensure that AIS security posture assessments, made in accordance with the DoD computer security program, are incorporated into NCSC goals and objectives.

5.6.10. Annually assess the overall AISs security posture and disseminate information on hostile threats against DoD AISs.

5.6.11. Operate a central technical center to provide, as requested, technical assistance to evaluate and certify the computer-based security features of AISs used in operational environments.

5.6.12. Prescribe the minimum security standards, methods, and procedures for safeguarding an AISs classified and sensitive technical security material, techniques, and information.

5.6.13. Review and approve standards, techniques, systems, and equipment for telecommunications and automated information systems security.

5.7. The Joint Chiefs of Staff (JCS) shall:

5.7.1. Implement an AIS security program under this Directive and SM-313-83 (reference (h)) for AISs of DoD Components and their contractors that handle SIOP-ESI.

5.7.2. Provide a source of education and training for managers in AIS security through the Department of Defense Computer Institute (DoDCI) of the National Defense University (NDU) (DoD Directive 5200.2 (reference (p))).

5.8. The Heads of DoD Components shall:

5.8.1. Implement and maintain an overall AIS security program designed to ensure compliance with this Directive.

5.8.2. Ensure that contractual requirements to protect classified and sensitive unclassified information are provided to their contractors.

5.8.3. Ensure that funding and resources are programmed for staffing, training, and supporting for this AIS security program and for implementation of AISs safeguards, as required, within the DoD Component.

5.8.4. Assign official(s) as the DAA (e.g., senior AIS policy official) responsible for accrediting each AIS under his or her jurisdiction and for ensuring compliance with AIS security requirements.

5.8.5. Establish and maintain an AIS security training and awareness program for all DoD military, civilian, and contractor personnel requiring access to AISs.

5.8.6. Ensure that periodic independent reviews of the security and protection of their AISs are done to ensure compliance with stated AIS security goals. Such reviews may be done using the procedures in DoD Directive 5010.38 (reference (q)).

5.8.7. Support the Computer Security Technical Vulnerability Reporting Program in accordance with DoD Instruction 5215.2 (reference (i)).

5.9. Each Designated Approving Authority (DAA) shall:

5.9.1. Review and approve security safeguards of AISs and issue accreditation statements for each AIS under the DAA's jurisdiction based on the acceptability of the security safeguards for the AIS.

5.9.2. Ensure that all the safeguards required, as stated in the accreditation documentation for each AIS, are implemented and maintained.

5.9.3. Identify security deficiencies and, where the deficiencies are serious enough to preclude accreditation, take action (e.g., allocate additional resources) to achieve an acceptable security level.

5.9.4. Ensure that an Information System Security Officer (ISSO) is named for each AIS, and that he or she receives applicable training to carry out the duties of this function. It is recommended that the ISSO not report to operational elements of the AIS over which security requirements of this Directive must be enforced.

5.9.5. Require that an AIS security education and training program be in place.

5.9.6. Ensure that data ownership is established for each AIS, to include accountability, access rights, and special handling requirements.

5.10. Each Information System Security Officer (ISSO) shall:

5.10.1. Ensure that the AIS is operated, used, maintained, and disposed of in accordance with internal security policies and practices.

5.10.2. Have the authority to enforce security policies and safeguards on all personnel having access to the AIS for which the ISSO has cognizance.

5.10.3. Ensure that users have the required personnel security clearances, authorization and need-to-know, have been indoctrinated, and are familiar with internal security practices before access to the AIS.

5.10.4. Ensure that audit trails are reviewed periodically.

5.10.5. Begin protective or corrective measures if a security problem exists.

5.10.6. Report security incidents in accordance with DoD 5200.1-R (reference (b)) and to the DAA when an AIS is involved.

5.10.7. Report the security status of the AIS, as required by the DAA.

5.10.8. Evaluate known vulnerabilities to ascertain if additional safeguards are needed.

5.10.9. Maintain a plan for system security improvements and progress towards meeting the accreditation.

6. EFFECTIVE DATE AND IMPLEMENTATION

6.1. This Directive is effective immediately.

6.2. Accreditations made using the requirements of the previous version of this Directive remain valid, but shall be updated within 3 years from the date of this Directive.

6.3. AISs that have started the design phase of the life-cycle process before the date of this Directive shall be accredited within 3 years of that date or before initial operational capability.

6.4. Each DoD Component Head shall forward an implementation plan for compliance with this Directive to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) within 180 days of the date of this Directive. This Directive shall be implemented without new DoD Component issuances.

Enclosures - 5

1. References, continued

2. Definitions

3. Minimum Security Requirements

4. Procedure for Determining Minimum AIS Computer-Based Security Requirements

5. Network Considerations

E1. ENCLOSURE 1

REFERENCES, continued

(e) National Communication Security Instruction 5004, "TEMPEST Countermeasures for Facilities Within the United States," January 1, 1984

(f) National Communication Security Instruction 5005, "TEMPEST Countermeasures for Facilities Outside the United States," January 1, 1984

(g) Director of Central Intelligence Directive Number 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks (U)," January 4, 1983

(h) SM-313-83, "Safeguarding the Single Integrated Operational Plan (U)," May 10, 1983

(i) DoD Instruction 5215.2, "Computer Security Technical Vulnerability Reporting Program," September 2, 1986

(j) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," December 12, 1985

(k) DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985,

authorized by DoD Directive 5200.28, December 18, 1972

(l) DoD Directive 7920.1, "Life-Cycle Management of Automated Information Systems (AIS)," October 17, 1978

(m) DoD Instruction 5210.74, "Security of DoD Contractor Telecommunications," June 26, 1985

(n) DoD Directive 5220.22, "Industrial Security Program," November 1, 1986

(o) DoD Regulation 5220.22-R, "Industrial Security Regulation," December 1985, authorized by DoD Directive 5220.22, December 8, 1980

(p) DoD Directive 5200.2, "DoD Personnel Security Program," December 20, 1979

(q) DoD Directive 5010.38, "Internal Management Control Program," July 16, 1984

(r) Executive Order 12356, "National Security Information," April 6, 1982

(s) DoD Directive 5230.24, "Distribution Statement on Technical Documents," March 18, 1987

(t) DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by DoD Directive 5200.28, December 18, 1972

(u) CSC-STD-003-85, "Computer Security Requirements," June 25, 1985

(v) NSC-TG-005, Version 1, "Trusted Network Interpretations," July 31, 1987

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Access. A specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., an AIS resource such as a record, file, program, output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information.

E2.1.2. Accountability. The property that enables activities on an AIS to be traced to individuals who may then be held responsible for their actions.

E2.1.3. Accreditation. A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

Accreditation is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations.

The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

E2.1.4. AIS Security. Measures and controls that safeguard or protect an AIS against unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data, and denial of service. AIS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards

needed to provide an acceptable protection level for an AIS and for data handled by an AIS.

E2.1.5. Assurance. A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation.

E2.1.6. Audit. An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

E2.1.7. Audit Trail. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

E2.1.8. Automated Information Systems (AISs). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

E2.1.9. Category. A grouping of classified or sensitive unclassified information to which an additional restrictive label is applied for signifying that personnel are granted access to the information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information).

E2.1.10. Certification. The technical evaluation of an AISs security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular AIS design and implementation meet a set of specified security requirements.

E2.1.11. Classified Information. Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; and (b) determined under E.O. 12356 (reference (r)), or prior orders, DoD 5200.1-R (reference (b)), to require protection against unauthorized disclosure; and so designated.

E2.1.12. Computer. A machine capable of accepting, performing calculations on, or otherwise manipulating or storing data. It usually consists of arithmetic and logical unit, and a control unit, and may have input and output devices and storage devices.

E2.1.13. Data. A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an AIS.

E2.1.14. Data Integrity. The state that exists when data is unchanged from its source and accidentally or maliciously has not been modified, altered, or destroyed.

E2.1.15. Data Owner. The authority, individual, or organization who has original responsibility for the data by statute, Executive order, or Directive.

E2.1.16. Dedicated Security Mode. A mode of operation wherein all users have the clearance or authorization and need-to-know for all data handled by the AIS. If the AIS processes special access information, all users require formal access approval. In the dedicated mode, an AIS may handle a single classification level

and/or category of information or a range of classification levels and/or categories.

E2.1.17. Denial of Service. Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability.

E2.1.18. Designated Approving Authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level, have authority to evaluate the overall mission requirements of the AIS, and to provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS.

E2.1.19. Embedded System. An embedded system is one that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem (e.g., ground support equipment, flight simulators, engine test stands, or fire control systems).

E2.1.20. Evaluated Products List (EPL). A documented inventory of equipments, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DoD 5200.28-STD (reference (k)).

E2.1.21. Features. (See Security Features, definition E2.1.40., below.)

E2.1.22. Formal Access Approval. Documented approval by a data owner to allow access to a particular category of information.

E2.1.23. Handled By. The term "handled by" denotes the activities performed on data in an AIS, such as collecting, processing, transferring, storing, retrieving, sorting, transmitting, disseminating, and controlling.

E2.1.24. Information. Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.

E2.1.25. Information System. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

E2.1.26. Information System Security Officer (ISSO). The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the concept development phase through its design, development, operation, maintenance, and secure disposal.

E2.1.27. Intelligent Terminal. A terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics.

E2.1.28. Multilevel Security Mode. A mode of operation that allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS.

E2.1.29. Need-to-Know. A determination made in the interest of U.S. national security by the custodian of classified or sensitive unclassified information, which a prospective recipient has a requirement for

access to, knowledge of, or possession of the information to perform official tasks or services.

E2.1.30. Network. A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

E2.1.31. Orange Book Terminology. Reference (k), also called the Orange Book, classifies AISs into four broad hierarchical divisions of security protection. Within divisions C and B there are further subdivisions called classes. These classes also are ordered in a hierarchical manner characterized by the set of computer security features they possess (see Security Features, definition E2.1.40., below).

E2.1.32. Partitioned Security Mode. A mode of operation wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by the AIS. This security mode encompasses the compartmented mode defined in DCID No. 1/16, reference (g).

E2.1.33. Periods Processing. A manner of operating an AIS in which the security mode of operation and/or maximum classification of data handled by the AIS is established for an interval of time (or period) and then changed for the following interval of time. A period extends from any secure initialization of the AIS to the completion of any purging of sensitive data handled by the AIS during the period.

E2.1.34. Purge. Removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is ensurance proportional to the sensitivity of the data that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge.

E2.1.35. Risk. A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

E2.1.36. Risk Analysis. An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

E2.1.37. Risk Index. The disparity between the minimum clearance or authorization of AIS users and the maximum sensitivity (e.g., classification and categories) of data handled by the AIS.

E2.1.38. Risk Management. The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.

E2.1.39. Safeguards. (See Security Safeguards, definition E2.1.42., below.)

E2.1.40. Security Features. The security-relevant functions, mechanisms, and characteristics of AIS hardware and software (e.g., identification, authentication, audit trail, access control).

E2.1.41. Security Mode. A mode of operation in which the DAA accredits an AIS to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, and partitioned) are restrictions on the

user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the AIS.

E2.1.42. Security Safeguards. The protective measures and controls that are prescribed to meet the security requirements specified for an AIS. These safeguards may include, but are not necessarily limited to, hardware and software security features; operation procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices.

E2.1.43. Sensitive Compartmented Information (SCI). Classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director, Central Intelligence.

E2.1.44. Sensitive Unclassified Information. Any information the loss, misuse, or unauthorized access to, or modification of which, adversely might affect U.S. national interest, the conduct of DoD programs, or the privacy of DoD personnel (e.g., FOIA exempt information and information whose distribution is limited by DoD Directive 5230.24 (reference (s))).

E2.1.45. SIOP-ESI. An acronym for Single Integrated Operational Plan-Extremely Sensitive Information, a DoD Special Access Program.

E2.1.46. Special Access Program. Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know, or special lists of persons determined to have a need-to-know.

E2.1.47. System High Security Mode. A mode of operation wherein all users having access to the AIS possess a security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes special access information, all users must have formal access approval.

E2.1.48. Telecommunications. Under this Directive, a general term expressing data transmission between computing systems and remotely located devices via a unit that performs the necessary format conversion and controls the rate of transmission.

E2.1.49. Trusted Products. Products evaluated and approved for inclusion on the Evaluated Products List (EPL).

E2.1.50. Unclassified Information. Any information that need not be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost or susceptibility to fraud, waste, or abuse.

E2.1.51. Users. People or processes accessing an AIS either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

E3. ENCLOSURE 3

MINIMUM SECURITY REQUIREMENTS

E3.1.1. MINIMUM SECURITY REQUIREMENTS. The following minimum requirements shall be met through automated

or manual means in a cost-effective manner and integrated fashion:

E3.1.1 1. Accountability. There shall be in place safeguards to ensure each person having access to an AIS may be held accountable for his or her actions on the AIS. There shall be an audit trail providing a documented history of DAIS use. The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur. To fulfill this requirement, the manual and/or automated audit trail shall document the following:

E3.1.1.1.1. The identity of each person and device having access to the AIS.

E3.1.1.1.2. The time of the access.

E3.1.1.1.3. User activity sufficient to ensure user actions are controlled and open to scrutiny.

E3.1.1.1.4. Activities that might modify, bypass, or negate safeguards controlled by the AIS.

E3.1.1.1.5. Security-relevant actions associated with periods processing or the changing of security levels or categories of information.

DAAs shall cause a review to be made of audit trails associated with the AIS(s) over which the DAAs have cognizance to determine an adequate retention period for the audit information. The decision to require an audit trail of user access to a stand-alone, single-user AIS (e.g., personal computer (PC), memory typewriter, drafting machine) should be left to the discretion of the DAA.

E3.1.1.2. Access. There shall be in place an access control policy for each AIS. It shall include features and/or procedures to enforce the access control policy of the information within the AIS. The identify of each user authorized access to the AIS shall be established positively before authorizing access.

E3.1.1.3. Security Training and Awareness. There shall be in place a security training and awareness program with training for the security needs of all persons accessing the AIS. The program shall ensure that all persons responsible for the AIS and/or information, therein, and all persons who access the AIS are aware of proper operational and security-related procedures and risks.

E3.1.1.4. Physical Controls. AIS hardware, software, and documentation, and all classified and sensitive unclassified data handled by the AIS shall be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification (i.e., data integrity shall be maintained). The level of control and protection shall be commensurate with the maximum sensitivity of the information and shall provide the most restrictive control measures required by the data to be handled. This includes having personnel, physical, administrative, and configuration controls. Additionally, protection against denial of service of AIS resources (e.g., hardware, software, firmware, and information) shall be consistent with the sensitivity of the information handled by the AIS. Unclassified hardware, software, or documentation of an AIS shall be protected if access to such hardware, software, or documentation reveals classified information, or access provides information that may be used to eliminate, circumvent, or otherwise

render ineffective the security safeguards for classified information. Software development and related activities (e.g., systems analysis) shall be controlled by physical controls (e.g., two-person control) and protected when it is determined that the software shall be used for handling classified or sensitive unclassified data.

E3.1.1.5. Marking. Classified and sensitive unclassified output shall be marked to accurately reflect the sensitivity of the information. Requirements for security classification and applicable markings for classified information are set forth in DoD 5200.1-R (reference (b)). The marking may be automated (i.e., the AIS has a feature that produces the markings) or may be done manually. Automated markings on output must not be relied on to be accurate, unless the security features and assurances of the AIS meet the requirements for a minimum security class B1 as specified in DoD 5200.28-STD (reference (k)). If B1 is not met, but automated controls are used, all output shall be protected at the highest classification level of the information handled by the AIS until manually reviewed by an authorized person to ensure that the output was marked accurately with the classification and caveats. All media (and containers) shall be marked and protected commensurate with the requirements for the highest security classification level and most restrictive category of the information ever stored until the media are declassified (e.g., degaussed or erased) using a DoD-approved methodology set forth in the DoD AIS Security Manual, DoD 5200.28-M (reference (t)), or unless the information is declassified or downgraded in accordance with reference (b).

E3.1.1.6. Least Privilege. The AIS shall function so that each user has access to all of the information to which the user is entitled (by virtue of clearance, formal access approval), but to no more. In the case of "need-to-know" for classified information, access must be essential for accomplishment of lawful and authorized Government purposes.

E3.1.1.7. Data Continuity. Each file or data collection in the AIS shall have an identifiable source throughout its life cycle. Its accessibility, maintenance, movement, and disposition shall be governed by security clearance, formal access approval, and need-to-know.

E3.1.1.8. Data Integrity. There shall be safeguards in place to detect and minimize inadvertent modification or destruction of data, and detect and prevent malicious destruction or modification of data.

E3.1.1.9. Contingency Planning. Contingency plans shall be developed and tested in accordance with OMB Circular No. A-130 (reference (j)) to ensure that AIS security controls function reliably and, if not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. If data is modified or destroyed, procedures must be in place to recover.

E3.1.1.10. Accreditation. Each AIS shall be accredited to operate in accordance with a DAA-approved set of security safeguards.

E3.1.1.11. Risk Management. There should be in place a risk management program to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.

E4. ENCLOSURE 4

PROCEDURE FOR DETERMINING MINIMUM AIS COMPUTER-BASED SECURITY REQUIREMENTS

E4.1.1. RISK ASSESSMENT PROCEDURE. The following risk assessment procedure is extracted from CSC-STD-003-85 (reference (u)). The procedure is used to determine the minimum evaluation class required for an AIS, based on the sensitivity of the information present in the AIS and on the clearances of its users. Any DoD Component desiring to use a different method to accomplish the intent of this enclosure may do so, if prior approval has been granted by the ASD(C3I).

NOTE: In the case of a network, the procedure is applied individually to each of the AISs in the network. The resulting evaluation class should be taken as a minimum partial requirement since connection of an AIS to another AIS or to a network may result in additional risks (see enclosure E5.). The DAA for a network also may decide to apply the procedure once for the network, and determine the evaluation class by applying the requirements in DoD 5200.28-STD (reference (k)) to the network as a whole.

E4.1.1.1. Step 1. Determine System Security Mode of Operation. The system security mode of operation for an AIS is determined as follows:

E4.1.1.1.1. An AIS is defined as operating in the dedicated security mode if all users have the clearance or authorization, documented formal access approval, if required, and the need-to-know for all information handled by the AIS. The AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. The AIS shall be isolated electrically, logically, and physically from all personnel and AISs not possessing the requisite clearance or authorization, formal access approval, if required, and need-to-know for all of the information handled by the AIS.

E4.1.1.1.2. An AIS is defined as operating in the system high security mode if all users have the clearance or authorization and documented formal access approval, if required, but not necessarily the need-to-know for all information handled by the AIS.

E4.1.1.1.3. An AIS is defined as operating in the multilevel security mode if not all users have the clearance, authorization, or formal access approval, if required, for all information handled by the AIS.

E4.1.1.1.4. An AIS is defined as operating in the partitioned security mode if all users possess the clearance, but not necessarily a formal access approval, for all information handled by the AIS.

E4.1.1.2. Step 2. Determine Minimum User Clearance or Authorization Rating. The minimum user clearance or authorization (Rmin) is defined as the maximum clearance or authorization of the least cleared or authorized user. Rmin is determined from Table E4.T1. The clearances used in the following table are defined in DoD Directive 5200.2 (reference (p)).

TABLE E4.T1.

MINIMUM USER CLEARANCE OR AUTHORIZATION SCALE

Rating

Uncleared OR Not Authorized (U)

0

Not Cleared but Authorized Access to Sensitive Unclassified Information (N)

1

Confidential (C)

2

Secret (S)

3

Top Secret (TS) and/or Current Background Investigation (BI)

4

Top Secret (TS) and/or Current Special Background Investigation (BI)

5

One Category (1C)

6

Multiple Categories (MC)

7

E4.1.1.3. Step 3. Determine Maximum Data Sensitivity Rating. The maximum data sensitivity (Rmax) is determined from the following table:

TABLE E4.T2.

MAXIMUM DATA SENSITIVITY SCALE

Maximum

Sensitivity Ratings 2

Without Categories

Rating

Maximum Data Sensitivity With Categories 1

Rating

(Rmax)

(Rmax)

(Rmax)

Unclassified (U)

0

Not Applicable 3

Not Classified but Sensitive 4

1

N With One or More Categories

2

Confidential (C)

2

C With One or More Categories

3

Secret (S)

3

S With One or More Categories

With No More Than One Category Containing

Secret Data

S With Two or More Categories Containing

Secret Data

4

5

Top Secret (TS)

5 5

TS With One or More Categories

With No More Than One Category Containing

Secret or Top Secret Data

TS With Two or More Categories Containing

Secret or Top Secret Data

6

7

_____

1 The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level. Systems in which all data is in the same category are treated as without categories.

2 Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

3 Unclassified data by definition may not contain categories.

4 Examples of N data include financial, proprietary, privacy, and mission-sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission-sensitive data), a higher rating may be warranted. Table E4.T2. prescribes minimum ratings.

5 The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes EXCEPTIONALLY GRAVE damage to U.S. national security, whereas the loss of Secret data causes SERIOUS damage.

E4.1.1.4. Step 4. Determine Risk Index. The risk index depends on the rating associated with the AIS minimum user clearance (Rmin) and the rating associated with the maximum classification of the information handled by the AIS (Rmax).

The risk index is computed as follows:

E4.1.1.4.1. Case a. If Rmin is less than Rmax, then the risk index is determined by subtracting Rmin from Rmax.

Risk Index = Rmax - Rmin

NOTE: There is one anomalous value that results because there are two "types" of Top Secret clearance and only one "type" of Top Secret data. When the minimum user clearance is TS/BI and the maximum data sensitivity is Top Secret without categories, then the risk index is 0 (rather than the value 1, which should result from a straight application of the formula).

E4.1.1.4.2. Case b. If Rmin is greater than or equal to Rmax, then:

Risk Index = 1, if there are categories to which some users are not authorized access, or:

Risk Index = 0, in all other cases.

E4.1.1.5. Step 5. Determine Minimum Security Evaluation Class For Computer-Based Controls.

E4.1.1.5.1. The following table shall be used to determine the minimum security class required for an AIS based on the computed risk index in Step 4, above. The levels in the table are those described in DoD 5200.28-STD (reference (k)).

TABLE E4.T3.

COMPUTER SECURITY REQUIREMENTS SCALE

Risk Index

Security Mode

Minimum Security Class 4

0

Dedicated 5

No minimum class 1,2

0

System High

C2 2

1

Multilevel,

B1 3

Partitioned

2

Multilevel,

B2

Partitioned

3

Multilevel

B3

4

Multilevel

A1

5

Multilevel

*

6

Multilevel

*

7

Multilevel

*

_____

1 Although there is no prescribed minimum class, the integrity and denial of service requirements of many systems warrant at least class C1 protection.

2 Automated markings on output must not be relied on to be accurate unless at least class B1 is used. (See requirements for marking in enclosure E3.)

3 Where an AIS handles classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being handled, at least a class B2 is required.

4 The asterisk (*) indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology.

5 Most embedded systems and desk top computers operate in the dedicated mode.

E4.1.1.6. Step 6. Adjustments to Computed Security Evaluation Class Required. Additional requirements or recommendations relevant to determining the minimum evaluation class include the following:

E4.1.1.6.1. Where an AIS is connected to a network or to another AIS, care should be taken to ensure that the requirements for accreditation of the AIS are not violated due to the presence of the network technology.

E4.1.1.6.2. In the dedicated mode where the AIS is connected to a network or to another AIS, it is recommended (although not required) that at least level CI be used. This recommendation is made because level C1 might provide a measure of security sufficient to prevent users from accidentally altering or deleting each other's data.

E4.1.1.6.3. An AIS using periods processing (i.e., operating in one or more security modes and/or at one or more security levels for certain periods of time where acceptable sanitization procedures are implemented between processing periods) may have more than one risk index. In such cases, the highest value of risk index shall be used in determining the minimum security feature level.

E5. ENCLOSURE 5

NETWORK CONSIDERATIONS

E5.1.1. For purposes of accreditation, a network shall be treated as either an interconnection of accredited AISs (which may be networks) or as a unified network. These two cases are discussed below:

E5.1.1.1. Case I. Interconnections of Accredited AISs

E5.1.1.1.1. If a network consists of previously accredited AISs, an MOA is required between the DAA of each DoD Component AIS and the DAA responsible for the network (as provided in section 4. of this Directive). The network DAA must ensure that interface restrictions and limitations are observed for connections between DoD Component AISs. The NCSC-TG-005 (reference (v)) provides interface restriction and limitation that may be applicable. In particular, connections between accredited AISs must be consistent with the mode of operation of each AIS, the specific sensitivity level or range of sensitivity levels for which each AIS is accredited, any additional interface constraints associated with the particular interface device used for the connection, and any other restrictions required by the MOA.

E5.1.1.1.2. Each AIS shall be assigned an accreditation range, consisting of the set of security levels that may be associated with data it sends over the network connection. If the accreditation range is more than a single level, the AIS reliably must segregate data by level within its accreditation range, and label it accurately for transmission over multilevel interfaces.

E5.1.1.1.3. DAAs of DoD Component AISs should be aware that connection to a network may involve additional risks because of the potential exposure of data in their own AIS to the larger community of all users of AISs

in the network. In connections to adjacent AISs, the operational modes and security mechanisms of those AISs should be taken into consideration, beyond the simple fact of their accreditation.

E5.1.1.1.4. Untrusted, unaccredited AISs, either individual computer systems or subnetworks, also may be components of a network. Connections between them and other component AISs are permissible under the same conditions in paragraph E5.1.1.1.1., above. Only unclassified information, which does not include sensitive unclassified information, may be sent to and from the untrusted, unaccredited AISs.

E5.1.1.1.5. Special AISs or support, such as packet switching nodes and terminal access interfaces, also must have received individual accreditation if they carry classified or sensitive unclassified information. The network DAA serves as the DAA for all such AISs.

E5.1.1.2. Case II. Unified Networks

E5.1.1.2.1. Some networks may be accredited as a whole without prior accreditation of each of their component AISs. It is necessary to treat a network as unified when some of its component AISs are so specialized or dependent on other components of the network for security support that individual accreditation of such components is not possible or meaningful with respect to secure network operation. In order to be accredited, a unified network shall possess a coherent network security architecture and design, and it should be developed with an attention to security requirements, mechanisms, and assurances commensurate with the range of sensitivity of information for which it is to be accredited.

E5.1.1.2.2. The recommended approach for accrediting a unified network is to apply enclosure E4. to the entire network to derive an evaluation class. Requirements to meet that evaluation class then are obtained from an applicable interpretation of DoD 5200.28-STD (reference (k)), such as NCSC-TG-005 (reference (v)).

SORT: 5200.30

DOCI: DODD 5200.30

DATE: 19830321

TITL: DODD 5200.30 Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records, March 21, 1983, USD(P)

Refs:(a) DoD Directive 5200.30, "Guidelines for Systematic Review of 20-Year-Old Classified Information in Permanently Valuable DoD Records," September 9, 1981 (hereby canceled)
(b) Executive Order 12356, "**National** Security Information," April 2, 1982
(c) Information Security Oversight Office Directive No. 1 Concerning **National** Security Information, June 23, 1982
(d) through (g), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a); establishes procedures and assigns responsibilities for the systematic declassification review of information classified under references (b) and (c), DoD Directive 5200.1 and DoD 5200.1-R (references (d) and (e)), and prior orders, directives, and regulations governing security classification; and implements section 3.3 of reference (b).

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD) and to activities assigned to the OSD for administrative support, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

2. This Directive applies to the systematic review of permanently valuable classified information, developed by or for the Department of Defense and its Components, or its predecessor components and activities, that is under the exclusive or final original classification jurisdiction of the Department of Defense.

3. Its provisions do not cover Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954 (reference (f)) or information in nonpermanent records.

4. Systematic declassification review of records pertaining to intelligence activities (including special activities) or intelligence sources or methods shall be in accordance with special procedures issued by the Director of Central Intelligence.

C. DEFINITIONS

1. Cryptologic Information. Information pertaining to or resulting from

the activities and operations involved in the production of signals intelligence (SIGINT) or to the maintenance of communications security (COMSEC).

2. Foreign Government Information. Information that is provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both are to be held in confidence; or produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof requiring that the information, the arrangement, or both are to be held in confidence*

3. Intelligence Method. Any process, mode of analysis, means of gathering data, or processing system or equipment used to produce intelligence.

4. Intelligence Source. A person or technical means that provides intelligence.

D. POLICY

It is the policy of the Department of Defense to assure that information that warrants protection against unauthorized disclosure is properly classified and safeguarded as well as to facilitate the flow of unclassified information about DoD operations to the public.

E. PROCEDURES

1. DoD classified information that is permanently valuable, as defined by 44 U.S.C. 2103 (reference (g)), that has been accessioned into the **National** Archives of the United States, will be reviewed systematically for declassification by the Archivist of the United States, with the assistance of the DoD personnel designated for that purpose, as it becomes 30 years old; however, file series concerning intelligence activities (including special activities) created after 1945, intelligence sources or methods created after 1945, and cryptology records created after 1945 will be reviewed as they become 50 years old.

2. All other DoD classified information and foreign government information that is permanently valuable and in the possession or control of DoD Components, including that held in federal records centers or other storage areas, may be reviewed systematically for declassification by the DoD Component exercising control of such information.

3. DoD classified information and foreign government information in the possession or control of DoD Components shall be declassified when they become 30 years old, or 50 years old in the case of DoD intelligence activities (including special activities) created after 1945, intelligence sources or methods created after 1945, or cryptology created after 1945, if they are not within one of the categories specified in enclosure 2 or 3.

4. Systematic review for declassification shall be in accordance with procedures contained in DoD 5200.1-R (reference (e)). Information that falls within any of the categories in enclosures 2 and 3 shall be

declassified if the designated DoD reviewer determines, in light of the declassification considerations contained in enclosure 4, that classification no longer is required. In the absence of such a declassification determination, the classification of the information shall continue as long as required by **national** security considerations.

5. Before any declassification or downgrading action, DoD information under review should be coordinated with the Department of State on subjects cited in enclosure 5, and with the Central intelligence Agency (CIA) on subjects cited in enclosure 6.

F. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy shall:

a. Exercise oversight and policy supervision over the implementation of this Directive.

b. Request DoD Components to review enclosures 2 and 4 of this Directive every 5 years.

c. Revise enclosures 2 and 4 to ensure they meet DoD needs.

d. Authorize, when appropriate, other federal agencies to apply this Directive to DoD information in their possession.

2. The Head of each DoD Component shall:

a. Recommend changes to the enclosures of this Directive.

b. Propose, with respect to specific programs, projects, and systems under his or her classification jurisdiction, supplements to enclosures 2 and 4 of this Directive.

c. Provide advice and designate experienced personnel to provide timely assistance to the Archivist of the United States in the systematic review of records under this Directive.

3. The Director, **National** Security Agency/Chief, Central Security Service (NSA/CSS), shall develop, for approval by the Secretary of Defense, special procedures for systematic review and declassification of classified cryptologic information.

4. The Archivist of the United States is authorized to apply this Directive when reviewing DoD classified information that has been accessioned into the Archives of the United States.

G. EFFECTIVE DATE

This Directive is effective immediately.

PAUL THAYER Deputy Secretary of Defense

Enclosures - 6 I. References 2. Categories of Information That Require Review Before Declassification 3. General Guidelines for Systematic Declassification Review of Foreign Government Information 4.

Declassification Considerations 5. Department of State Areas of Interest

6. Central Intelligence Agency Areas of Interest

REFERENCES, continued

(d) DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982

(e) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, June 7, 1982

(f) Public Law 83-703, Atomic Energy Act of 1954

(g) Title 44, United States Code, Section 2103

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION

The following categories of information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive:

1. Nuclear propulsion information.

2. Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System.

3. Information concerning the safeguarding of nuclear materials or facilities.

4. Information that could affect the conduct of current or future U.S. foreign relations. (Also see enclosure 5.)

5. Information that could affect the current or future military usefulness of policies, programs, weapon systems, operations, or plans when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operations plans.

6. Research, development, test, and evaluation (RDT&E) of chemical and biological weapons and defensive systems; specific identification of chemical and biological agents and munitions; chemical and biological warfare plans; and U.S. vulnerability to chemical or biological warfare attack.

7. Information about capabilities, installations, exercises, research, development, testing and evaluation, plans, operations, procedures, techniques, organization, training, sensitive liaison and relationships, and equipment concerning psychological operations; escape, evasion, rescue and recovery, insertion, and infiltration and exfiltration; cover and support; deception; unconventional warfare and special operations; and the personnel assigned to or engaged in these activities.

8. Information that reveals sources or methods of intelligence or counterintelligence, counterintelligence activities, special activities, identities of clandestine human agents, methods of special operations, analytical techniques for the interpretation of intelligence data, and foreign intelligence reporting. This includes information that reveals theoverall scope, processing rates, timeliness, and accuracy of intelligence systems and networks, including the means of interconnecting such systems and networks and their vulnerabilities.

9. Information that relates to intelligence activities conducted jointly

by the Department of Defense with other federal agencies or to intelligence activities conducted by other federal agencies in which the Department of Defense has provided support. (Also see enclosure 6.)

10. Airborne radar and infrared imagery.

11. Information that reveals space system:

a. Design features, capabilities, and limitations (such as antijam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters).

b. Concepts of operation, orbital characteristics, orbital support methods, network configurations, deployments, ground support facility locations, and force structure.

12. Information that reveals operational communications equipment and systems:

a. Electronic counter-countermeasures (ECCM) design features or performance capabilities.

b. Vulnerability and susceptibility to any or all types of electronic warfare.

13. Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures (ECM), and ECCM) or related activities, including:

a. Information concerning or revealing nomenclatures, functions, technicalcharacteristics, or descriptions of foreign communications and electronic equipment, its employment or deployment, and its association with weapon systems or military operations.

b. Information concerning or revealing the processes, techniques, operations, or scope of activities involved in acquiring, analyzing, and evaluating the above information, and the degree of success obtained.

14. Information concerning Department of the Army systems listed in attachment 1.

15. Information concerning Department of the Navy systems listed in attachment 2.

16. Information concerning Department of the Air Force systems listed in attachment 3.

17. Cryptologic information (including cryptologic sources and methods). This includes information concerning or revealing the processes, techniques, operations, and scope of SIGINT comprising communications intelligence, electronics intelligence, and telemetry intelligence; and the cryptosecurity and emission security components of COMSEC, including the communications portion of cover and deception plans.

a. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

(1) Those that relate to COMSEC. In documentary form, they provide COMSEC guidance or information. Many COMSEC documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing transmission security (TSEC) nomenclature and crypto keying material for use in enciphering communications and other COMSEC documentation such as **National** COMSEC Instructions, **National** COMSEC/Emanations Security (EMSEC) Information Memoranda, **National** COMSEC Committee Policies, COMSEC Resources Program documents, COMSEC Equipment Engineering Bulletins, COMSEC Equipment System Descriptions, and COMSEC Technical Bulletins.

(2) Those that relate to SIGINT. These appear as reports in various formats that bear security classifications, sometimes followed by five-letter codewords (World War II's ULTRA, for example) and often carrying warning caveats such as "This document contains codeword material" and "Utmost secrecy is necessary.. ." Formats may appear as messages having addressees, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

(3) RDT&E reports and information that relate to either COMSEC or SIGINT.

b. Commonly used words that may help in identification of cryptologic documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signals intelligence" or "SIGINT," "signal security," and "TEMPEST."

Attachments - 3 1. Department of the Army Systems 2. Department of the Navy Systems 3. Department of the Air Force Systems

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION
DEPARTMENT OF THE ARMY SYSTEMS

The following categories of Army information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive.

1. Ballistic Missile Defense (BMD) missile information, including the principle of operation of warheads (fuzing, arming, firing, and destruct operations); quality or reliability requirements; threat data; vulnerability; ECM and ECCM; details of design, assembly, and construction; and principle of operations.

2. BMD systems data, including the concept definition (tentative roles, threat definition, and analysis and effectiveness); detailed quantitative technical system description-revealing capabilities or unique weaknesses that are exploitable; overall assessment of specific threat-revealing vulnerability or capability; discrimination technology; and details of operational concepts.

3. BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.

4. Shaped-charge technology.

5. Fleshettes.

6. M380 Beehive round.

7. Electromagnetic propulsion technology.

8. Space weapons concepts.

9. Radar-fuzing programs.

10. Guided projectiles technology.

11. ECM and ECCM to weapons systems.

12. Armor materials concepts, designs, or research.

13. 2.75-inch Rocket System.

14. Air Defense Command and Coordination System (AN/TSQ-51).

IS. Airborne Target Acquisition and Fire Control System.

16. Chaparral Missile System.

17. Dragon Guided Missile System Surface Attack, M47.

18. Forward Area Alerting Radar (FAAR) System.

19. Ground laser designators.

20. Hawk Guided Missile System.

21. Heliborne, Laser, Air Defense Suppression and Fire and Forget Guided Missile System (HELLFIRE).

22. Honest John Missile System.

23. Lance Field Artillery Missile System.

24. Land Combat Support System (LCSS).

25. M22 (55-11) Guided Missile System, Helicopter Armament Subsystem.

26. Guided Missile System, Air Defense (NIKE HERCULES with Improved Capabilities with HIPAR and ANTIJAM Improvement).

27. Patriot Air Defense Missile System.

28. Pershing IA Guided Missile System.

29. Pershing II Guided Missile System.

30. Guided Missile System, Intercept Aerial, M41 (REDEYE) and Associated

Equipment.

31. U.S. Roland Missile System.

32. Sergeant Missile System (less warhead) (as pertains to electronics and penetration aids only).

33. Shillelagh Missile System.

34. Stinger/Stinger-Post Guided Missile System (FIM-92A).

35. Terminally Guided Warhead (TWG) for Multiple Launch Rocket System (MLRS).

36. TOW Heavy Antitank Weapon System.

37. Viper Light Antitank/Assault Weapon System.

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION

DEPARTMENT OF THE NAVY SYSTEMS

The following categories of Navy information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive.

I. Naval nuclear propulsion information.

2. Conventional surface ship information:

a. Vulnerabilities of protective systems, specifically:

(1) Passive protection information concerning ballistic torpedo and underbottom protective systems.

(2) Weapon protection requirement levels for conventional, nuclear, biological, or chemical weapons.

(3) General arrangements, drawings, and booklets of general plans (applicable to carriers only).

b. Ship-silencing information relative to:

(1) Signatures (acoustic, seismic, infrared, magnetic (including alternating magnetic (AM)), pressure, and underwater electric potential (UEP)).

(2) Procedures and techniques for noise reduction pertaining to an individual ship's component.

(3) Vibration data relating to hull and machinery.

c. Operational characteristics related to performance as follows:

(1) Endurance or total fuel capacity.

(2) Tactical information, such as times for ship turning, zero to maximum

speed, and maximum to zero speed.

3. All information that is uniquely applicable to nuclear-powered surface ships or submarines.

4. Information concerning diesel submarines as follows:

a. Ship-silencing data or acoustic warfare systems relative to:

(1) Overside, platform, and sonar noise signature.

(2) Radiated noise and echo response.

(3) All vibration data.

(4) Seismic, magnetic (including AM), pressure, and UEP signature data.

b. Details of operational assignments, that is, war plans, antisubmarine warfare (ASW), and surveillance tasks.

c. General arrangements, drawings, and plans of SS563 class submarine hulls.

5. Sound Surveillance System (SOSUS) data.

6. Information concerning mine warfare, mine sweeping, and mine countermeasures.

7. ECM or ECCM features and capabilities of any electronic equipment.

8. Torpedo information as follows:

a. Torpedo countermeasures devices: T-MK6 (FANFARE) and NAE beacons.

b. Tactical performance, tactical doctrine, and vulnerability to countermeasures *

9. Design performance and functional characteristics of guided missiles, guided projectiles, sonars, radars, acoustic equipments, and fire control systems.

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION
DEPARTMENT OF THE AIR FORCE SYSTEMS

The Department of the Air Force has determined that the categories identified in enclosure 2 of this Directive shall apply to Air Force information.

(DATA OMITTED)

DE CLASSIFICATION CONSIDERATIONS

1. Technological developments; widespread public knowledge of the subject matter; changes in military plans, operations, systems, or equipment; changes in the foreign relations or defense commitments of the United States; and similar events may bear upon the determination of whether

information should be declassified. If the responsible DoD reviewer decides that, in view of such circumstances, the public disclosure of the information being reviewed no longer would result in damage to the **national** security, the information shall be declassified.

2. The following are examples of considerations that may be appropriate in deciding whether information in the categories listed in enclosure 2 may be declassified when it is reviewed:

a. The information no longer provides the United States a scientific, engineering, technical, operational, intelligence, strategic, or tactical advantage over other nations.

b. The operational military capability of the United States revealed by the information no longer constitutes a limitation on the effectiveness of the Armed Forces.

c. The information is pertinent to a system that no longer is used or relied on for the defense of the United States or its allies and does not disclose the capabilities or vulnerabilities of existing operational systems.

d. The program, project, or system information no longer reveals a currentweakness or vulnerability.

e. The information pertains to an intelligence objective or diplomatic initiative that has been abandoned or achieved and will no longer damage the foreign relations of the United States.

f. The information reveals the fact or identity of a U.S. intelligence source, method, or capability that no longer is employed and that relates to no current source, method, or capability that upon disclosure could cause damage to **national** security or place a person in immediate jeopardy.

g. The information concerns foreign relations matters whose disclosure canno longer be expected to cause or increase international tension to the detriment of the **national** security of the United States.

3. Declassification of information that reveals the identities of clandestine human agents shall be accomplished only in accordance with procedures established by the Director of Central Intelligence for that purpose.

4. The NSA/CSS is the sole authority for the review and declassification of classified cryptologic information. The procedures established by the NSA/CSS to facilitate the review and declassification of classified cryptologic information are:

a. COMSEC Documents and Materials

(1) If records or materials in this category are found in agency files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency concerned or by appropriate channels to the following address:

Director **National** Security Agency ATTN: Director of Policy (Q4) Fort George G. Meade, Maryland 20755

(2) If the COMSEC information has been incorporated into other documents by the receiving agency, referral to the NSA/CSS is necessary before declassification.

b. SIGINT Information

(1) If the SIGINT information is contained in a document or record originated by a DoD cryptologic organization, such as the NSA/CSS, and is in the files of a noncryptologic agency, such material will not be declassified if retained in accordance with an approved records disposition schedule. If the material must be retained, it shall be referred to the NSA/CSS for systematic review for declassification.

(2) If the SIGINT information has been incorporated by the receiving agency into documents it produces, referral to the NSA/CSS is necessary before any declassification.

DEPARTMENT OF STATE AREAS OF INTEREST

1. Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

2. Statements of U.S. intent militarily to attack in stated contingencies identifiable areas in any foreign country or region.

3. Statements of U.S. policies or initiatives within collective security organizations (for example, North Atlantic Treaty Organization (NATO) and Organization of American States (OAS)).

4. Agreements with foreign countries for the use of, or access to, military facilities.

5. Contingency plans insofar as they involve other countries, the use of foreign bases, territory or airspace, or the use of chemical, biological, or nuclear weapons.

6. Defense surveys of foreign territories for purposes of basing or use in contingencies.

7. Reports documenting conversations with foreign officials, that is, foreign government information.

CENTRAL INTELLIGENCE AGENCY AREAS OF INTEREST

1. Cryptologic, cryptographic, or STGINT. (Information in this category shall continue to be forwarded to the NSA/CSS in accordance with enclosure 4, paragraph 4. The NSA/CSS shall arrange for necessary coordination.)

2. Counterintelligence.

3. Special access programs.

4. Information that identifies clandestine organizations, agents, sources, or methods.

5. Information on personnel under official or nonofficial cover or

revelation of a cover arrangement.

6. Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods.

7. Methods or procedures used to acquire, produce, or support intelligence activities *

3. CIA structure, size, installations, security, objectives, and budget.

9. Information that would divulge intelligence interests, value, or extent of knowledge on a subject.

10. Training provided to or by the CIA that would indicate its capability or identify personnel.

11. Personnel recruiting, hiring, training, assignment, and evaluation policies.

12. Information that could lead to foreign political, economic, or military action against the United States or its allies.

13. Events leading to international tension that would affect U.S. foreign policy.

14. Diplomatic or economic activities affecting **national** security or international security negotiations.

15. Information affecting U.S. plans to meet diplomatic contingencies affecting **national** security.

16. Nonattributable activities conducted abroad in support of U.S. foreign policy.

17. U.S. surreptitious collection in a foreign nation that would affect relations with the country.

18. Covert relationships with international organizations or foreign governments.

19. Information related to political or economic instabilities in a foreign country threatening American lives and installations therein.

20. Information divulging U.S. intelligence collection and assessment capabilities.

21. U.S. and allies' defense plans and capabilities that enable a foreign entity to develop countermeasures.

22. Information disclosing U.S. systems and weapons capabilities or deployment.

23. Information on research, development, and engineering that enables the United States to maintain an advantage of value to **national** security.

24. Information on technical systems for collection and production of

intelligence, and their use.

25. U.S. nuclear programs and facilities.

26. Foreign nuclear programs, facilities, and intentions.

27. Contractual relationships that reveal the specific interest and expertise of the CIA.

28. Information that could result in action placing an individual in jeopardy.

29. Information on secret writing when it relates to specific chemicals, reagents, developers, and microdots.

30. Reports of the Foreign Broadcast Information Service (FBIS) (-- Branch, -- Division) between July 31, 1946, and December 31, 1950, marked CONFIDENTIAL or above.

31. Reports of the Foreign Documents Division between 1946 and 1950 marked RESTRICTED or above.

32. Q information reports.

33. FDD translations.

34. U reports.

Department of Defense

DIRECTIVE

NUMBER 5200.32

February 26, 1996

ASD(C3I)

SUBJECT: Department of Defense Security Countermeasures (SCM) and Polygraph Education, Training, and Program Support

References: (a) DoD Directive 5200.32, "Department of Defense Security Institute (DoDSI)," August 29, 1986 (hereby canceled)

(b) DoD Directive 5210.78, "Department of Defense Polygraph Institute (DoDPI)," September 18, 1991 (hereby canceled)

(c) DoD Directive 5210.48, "DoD Polygraph Program," December 24, 1984

(d) DoD Instruction 5240.5, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," May 23, 1984

(e) through (i), see enclosure E1.

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a);

1.2. Replaces reference (b);

1.3. Establishes policy and assigns responsibilities on DoD SCM and polygraph education, training, and program support.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Applies to contractors and their personnel.

2.3. Assigns education, training, and other functions supporting DoD SCM programs and DoD Directive 5210.48 (reference (c)). This includes management of all technical security training, including DoD technical surveillance countermeasures (TSCM) training consistent with DoD Instruction 5240.5 (reference (d)), conducted by or for the Interagency Training Center (ITC) training activity and for related DoD training conducted elsewhere and

training activities and functions available to contractors and contractor employees.

3. DEFINITIONS

3.1. Focal Point. A DoD Component-designated responsibility under this Directive to monitor existing and proposed education and/or training courses, seminars, conferences, or materials, having relevance to a particular SCM discipline, evaluating the quality of such courses or materials, and recommending to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)), through the Security Education Advisory Group (SEAG), those courses and/or materials that the focal point believes should be included in the master data base to be maintained by the Department of Defense Security Institute (DoDSI). A focal point shall also identify to the ASD(C3I), through the SEAG, those instances where quality education and/or training courses are required, but are not available, and make recommendations concerning the nature and content of education and/or training courses needed to fulfill.

3.2. Professional Development. Those aspects of career development concerned with the education and training of individuals to improve their performance in given positions and specialties.

3.3. Security Countermeasures (SCM). Those activities required to detect, deter, or prevent espionage, sabotage, theft, and unauthorized use of classified information, systems, or material as well as the physical protection of DoD personnel and other valuable assets.

3.4. Security Countermeasures (SCM) Education and Training. Those formal activities, products, and services intended to create or enhance the knowledge or skills of persons, or raise their level of motivation, performance, or awareness with respect to the protection of classified information, systems, or material as well as the physical protection of DoD personnel and other valuable assets.

3.5. Technical Security. The SCM; i.e., technical surveillance countermeasures, information systems security, and counter-signals intelligence, that operate against unauthorized intercept of unencrypted information during preparation or transmission and that use electronic and electro-mechanical devices to safeguard classified or controlled information and material.

4. POLICY

It is DoD policy that:

4.1. Uniform, standardized, effective, and cost-efficient education and training programs shall be established and maintained to meet national and DoD-level SCM objectives and both near-term and long-term professional development requirements of DoD civilian, military, and contractor personnel charged with the execution of SCM responsibilities.

4.2. DoDSI shall function as the primary resource for DoD SCM education, training, and professional development support. Where a DoD Component is assigned focal point responsibility for education and training for a particular SCM program, the nature and extent of support to be provided by the DoDSI shall be determined by the ASD(C3I) in coordination with the focal point. DoDSI shall establish and maintain a listing of recommended SCM education and training courses and materials that will be provided to DoD Components, DoD contractors, and other Federal Agencies upon request.

4.3. The DoD Polygraph Institute (DoDPI) shall function as the sole source for basic and advanced psychophysiological

detection of deception (PDD) education and training for DoD polygraph examiners and shall conduct an aggressive research program to ensure that the DoD PDD Program of Instruction takes advantage of the latest techniques and technology. DoDPI may support other Federal Agencies on either a reimbursable or space available basis.

4.4. Focal points designated under this Directive shall monitor and review education, training, and professional development courses and materials available in their respective areas of responsibility, and recommend to the SEAG those courses and materials they believe should be adopted for use by the DoD Components. Where a need for education and training support exists, but no courses and materials are currently available, focal points shall develop and submit to the SEAG recommendations for proposed courses and materials to meet requirements.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Oversee DoD SCM and polygraph education, training, and professional development programs to ensure that such programs focus on essential needs, avoid inefficiency and unwarranted redundancy, promote cooperation and mutual support, and recognize assigned authorities and responsibilities.

5.1.2. Have authority, direction, and control of the DoDSI and the DoDPI and ensure that these activities operate efficiently and that appropriate management safeguards are in place to prevent fraud, waste, and abuse.

5.1.3. Oversee and manage the activities of the ITC, including technical security training, research, operations, and program support. Technical security training responsibilities should be exercised with the coordination and participation of the U.S. Intelligence and SCM communities.

5.1.4. Ensure that the Director, Defense Investigative Service (DIS), provides the DoDSI, ITC and the DoDPI with funding approved by the ASD(C3I) and includes the DoDSI and DoDPI annual budgets as separate line items in the DIS budget and financial plan.

5.1.5. Serve as approval authority for requests for DoDSI services or products above and beyond those covered by the current DoDSI budget allocation and, consistent with DoD 7220.9-M and DoD 7000.14-R (references (e) and (f)), and establish such reimbursable authority and agreements as may be required to permit DoDSI to accept and obligate funds necessary to fulfill ASD(C3I)-approved requests.

5.1.6. Appoint the Chair, Joint Visual Information SCM Review Board, established under DoD Directive 5040.2 (reference (g)).

5.1.7. Establish, and appoint the Chair of, a DoDPI Advisory Committee consisting of the Polygraph Program Managers of the DoD Components and, as appropriate, other Federal Agencies. The committee shall meet at least annually to provide advice and assistance to the Director, DoDPI, on ongoing or proposed polygraph projects and other matters pertinent to the effective operation of the DoDPI.

5.1.8. Establish a SEAG, consisting of representatives from the DoD Components and, as appropriate, other Federal Agencies. This group will meet at least biannually and will serve as the DoD forum for the discussion of SCM education, training and professional development

support requirements. SEAG working groups and additional customer advisory bodies may be established as needed. Refer to DoD Directive 5105.4 (reference (h)) for guidance relating to advisory committees including individuals who are not full-time employees of the Federal Government.

5.1.9. Approve and publish DoD Instructions and Publications, as necessary, to guide and direct DoD SCM security education, training, and career development activities.

5.1.10. Encourage liaison among the DoD Components with SCM security education and training responsibilities and other DoD Components; industry; professional associations; academia; Federal, State, and local government organizations; and international organizations. The purpose of such liaison is to share information that may be of use in implementing or improving DoD SCM education, training, and professional development programs. If liaison includes establishing advisory committees, including individuals who are not full-time employees of the Federal Government, refer to DoD Directive 5105.4 (reference (h)) for guidance.

5.1.11. Establish policies and procedures on DoD SCM security education and training support to Federal, State, and local agencies and to foreign governments.

5.1.12. Ensure that the Director, Defense Intelligence Agency, serves as the focal point for sensitive compartmented information security education and training.

5.2. The Under Secretary of Defense for Acquisition and Technology shall ensure that the Director, Defense Logistics Agency, provides requisite administrative support for DoDSI's operations at the Defense General Supply Center, Richmond, VA. Such support shall be provided on a reimbursable basis in accordance with DoD Instruction 4000.19 (reference (i)).

5.3. The Under Secretary of Defense for Personnel and Readiness shall provide computer programming and analysis resources at the Defense Manpower Data Center to support the DoDSI, ITC, and DoDPI, as required, subject to availability of such resources or reimbursement from the requesting Agency.

5.4. The Under Secretary of Defense for Policy shall serve as the focal point for international programs and special access program security education, training, and professional development.

5.5. The Secretary of the Army shall:

5.5.1. Serve as the focal point for physical security education and training.

5.5.2. Provide such facility, administrative, logistic, and practical examination support as may be required to support the DoDPI mission.

5.6. The Director, National Security Agency, shall serve as the focal point for DoD communications security, cryptologic security, and, information systems security education and training.

5.7. The Inspector General of the Department of Defense shall serve as the focal point, in coordination with the ASD(C3I), for polygraph education and training as it applies to the investigation of criminal cases.

5.8. The Heads of the DoD Components shall:

5.8.1. Advise the ASD(C3I) of current and projected requirements for SCM education and training support.

5.8.2. Establish and maintain professional development programs to meet both the near-term and long-term requirements of civilian and military personnel charged with the execution of SCM responsibilities.

5.8.3. Provide resources to support their respective requests for SCM education and training products and services over and above those funded for in the responsible Component or DoD activity current budget allocation.

5.8.4. Within statutory and operational requirements governing criminal and other investigations, make available to the DoDPI all records, case files, and quality control information as required by the DoDPI to accomplish its mission.

6. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 1

1. References, continued

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD 7220.9-M, "Department of Defense Accounting Manual," February 1988, authorized by DoD Instruction 7220.9, October 22, 1981

(f) DoD 7000.14-R, "Department of Defense Financial Management Regulation," March 1993, authorized by DoD Instruction 7000.14, November 15, 1992

(g) DoD Directive 5040.2, "Visual Information," December 7, 1987

(h) DoD Directive 5105.4, "Department of Defense Federal Advisory Committee Management Programs," September 5, 1989

(i) DoD Instruction 4000.19, "Interservice, Interdepartmental, and Interagency Support," April 15, 1992

Department of Defense

DIRECTIVE

NUMBER 5200.33

December 7, 1994

Administrative Reissuance Incorporating Change 1, August 25, 1998

ASD(C3I)

SUBJECT: Defense Courier Service (DCS)

References: (a) DoD Directive 5200.33, subject as above, September 30, 1987 (hereby canceled)

(b) DoD 5200.33-R, "Defense Courier Service Regulation," current edition, authorized by this Directive

(c) DoD 5025. l-M. "DoD Directives System Procedures," August 1994, authored by DoD Directive 5025.1, June 24, 1994

(d) Chairman of the Joint Chiefs of Staff Instruction 3260.01, "Joint Policy Governing Positive Control Material and Devices," July 31, 1995

(e) through (i), see enclosure E1.

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policy and responsibilities for the DCS; establishes the DCS as a direct reporting unit under the Commander Air Mobility Command (CDR AMC); and authorizes the publication of reference (b), in accordance with reference (c).

2. APPLICABILITY AND SCOPE

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Uniformed Services University of the Health Sciences, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Other activities of the U.S. Government, U.S. Government contractors, foreign governments, and the North Atlantic Treaty Organization (NATO) seeking to use the services of the DCS.

3. POLICY

It is DoD policy that:

3.1. The DCS shall establish, staff, operate, and maintain an international network of couriers and courier stations

for the expeditious, cost-effective, and secure transmission of qualified classified documents and material. In all instances, the security of documents or material shall be the primary objective. The DoD Components and contractors shall, to the maximum extent possible, use the services of the DCS for transmission of qualified classified documents or material requiring escort by courier.

3.2. DCS users shall ensure that only qualified classified material is entered into the DCS system. Qualified and prohibited material are delineated in enclosure E2.

3.3. Outside the United States, qualified material shall be transported by the DCS only to or from those locations where the DCS has an established operational presence in support of U.S. Armed Forces and it has a reasonable assurance that DCS material will not be subject to search and seizure by foreign customs or other foreign officials. (The DCS transfers materials to the Department of State (DoS) for final delivery in foreign countries when that is not the case.) Requests to expand DCS service to other areas outside the United States must be approved by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)).

3.4. DCS support during contingencies or hostilities shall be provided in accordance with requirements of the Chairman of the Joint Chiefs of Staff and the Combatant Commanders.

3.5. The DCS system shall provide “two person control” only for that nuclear command and control materiel delineated in Chairman of the Joint Chiefs of Staff Instruction 3260.1 and Chairman of the Joint Chiefs of Staff Instruction 3231.01 (references (d) and (e)).

3.6. The Commander, DCS, shall be an officer (O-6 position) with selection made by the CDR AMC. The normal tour of duty for that position shall be 3 years.

4. RESPONSIBILITIES

4.1. The Assistant Secretary of Defense for Command, Control, Communication, and Intelligence shall:

4.1.1. Provide security policy and procedural guidance for the DCS operation through issuance of DoD Instructions, Regulations and other guidance, as required, and oversee implementation of such policies and procedures.

4.1.2. Authorize exceptions to this Directive. That authority may be delegated to the Deputy Assistant Secretary of Defense (Intelligence and Security), and a single designee.

4.2. The Heads of the DoD Components shall:

4.2.1. Coordinate their courier requirements and priorities with the DCS, including requirements of their contractors and Foreign Military Sales (FMS), consistent with DoD 7000.14-R (reference (f)).

4.2.2. Program and budget for requirements and reimburse the DCS for all services provided, including special delivery services.

4.2.3. Provide support in emergency situations to DCS couriers necessary to safeguard DCS shipments, in accordance with DoD Instruction 4000.19 (reference (g)).

4.2.4. Assess the responsiveness of the DCS to their operational needs and advise the CDR, AMC of any problem

areas.

4.3. The Secretaries of the Military Departments shall:

4.3.1. Ensure that qualified personnel are assigned to carry out the DCS mission.

4.3.2. In coordination with the DCS, and in accordance with reference (g)), provide, support, and maintain courier stations at locations determined to be consistent with mission requirements.

4.4. The Commander, Air Mobility Command, shall:

4.4.1. Exercise combatant command authority over the DCS.

4.4.2. Coordinate DCS operations, as appropriate, with other Commands and Agencies.

4.4.3. Keep the ASD(C3I) informed, through the Chairman of the Joint Chiefs of Staff, of significant matters about DCS activities.

4.4.4. Provide advice and recommendations on matters in the areas of responsibilities assigned to the DCS.

4.4.5. Establish program and budget requirements for normal operations and support costs of the DCS as part of the AMC Transportation Working Capital Fund (TWCF).

4.4.6. Provide for movement of qualified DCS material during war, contingencies, and other emergencies in accordance with priorities established with supported activities.

4.5. The Commanders of the Combatant Commands shall:

4.5.1. Coordinate with host-nation officials to develop and implement procedures for the protection of DCS material from search and seizure by their customs or other agency officials.

4.5.2. During wartime or contingency situations, identify priorities for material destined to his or her command based on mission and operational requirements and ensure that the DCS is accorded appropriate airlift priority to meet these requirements.

4.6. The Heads of Non-DoD U.S. Government Departments and Agencies that use the DCS shall:

4.6.1. Coordinate their courier requirements and priorities, including requirements of their sponsored contractors and the FMS, consistent with DoD 7000.14-R (reference (f)).

4.6.2. Provide support, in their respective fields of responsibility, to the Commander, DCS, as required to carry out the assigned mission of the DCS.

4.6.3. Assess the responsiveness of the DCS to their operational needs and advise the ASD(C3I) of any problem areas.

4.6.4. Budget for, and reimburse the DCS for, the services it provides, in accordance with 31 U.S.C. 1535 (reference (h)) unless otherwise provided by statute.

5. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. DoD 5200.33-R (reference (b)) constitutes implementation of this Directive.

1. References, continued

2. Qualified and Prohibited Material

E1. ENCLOSURE 1

REFERENCES, continued

(e) Chairman of the Joint Chiefs of Staff Instruction 3231.01, " Safeguarding the Single Integrated Operational Plan," November 30, 19932

(f) DoD 7000.14-R, "Department of Defense Financial Management Regulation (Security Assistance Policy and Procedures)," Volume 15, March 1993, authorized by DoD Instruction 7000.14, November 15, 1992

(g) DoD Instruction 4000.19, "Interservice, and Intragovernmental Support," August 9, 1995

(h) Section 1535 of title 31, United States Code

(i) Section 812 of title 21, United States Code

2 Available from the JCS Documents Division, Room 2B917, Pentagon, Washington, DC 20318-0400

E2. ENCLOSURE 2

QUALIFIED AND PROHIBITED MATERIAL

E2.1. QUALIFIED MATERIAL

The following categories of material qualify for DCS handling:

E2.1.1. DoD Material

E2.1.1.1. Top Secret information.

E2.1.1.2. Classified cryptographic and communication security material.

E2.1.1.3. Classified cryptologic material.

E2.1.1.4. Cryptographic keying material designated and marked "CRYPTO" by the National Security Agency.

E2.1.1.5. Sensitive Compartmented Information.

E2.1.1.6. Air and spaceborne imagery material classified SECRET or higher.

E2.1.1.7. Controlled cryptographic items for shipment outside the 48 contiguous States when no other means of secure transportation is available.

E2.1.1.8. FMS material, if otherwise qualified.

E2.1.1.9. Any U.S. classified material that cannot be transmitted in U.S. custody by any other means.

E2.1.1.10. Single Integrated Operational Plan material and SECRET or more highly classified operational and/or targeting support material.

E2.1.1.11. End of Cruise Data Packages.

E2.1.2. Other Qualified Material

E2.1.2.1. DoS-accompanied diplomatic courier pouches.

E2.1.2.2. Material in paragraphs E2.1.1.1. through

E2.1.1.9. of this enclosure, above, of other U.S. Government Agencies.

E2.1.2.3. Material in paragraphs E2.1.1.1. through E2.1.1.8., above, of NATO.

E2.1.2.4. Material in paragraphs E2.1.1.1. through E2.1.1.7., above, of foreign governments when used for combined operations.

E2.1.2.5. Material in paragraphs E2.1.1.1. through E2.1.1.9., above, of Federal Government contractors when specifically provided for in their contracts.

E2.2. PROHIBITED MATERIAL

The following material is not authorized entry into the DCS system, regardless of classification or other qualifying criteria:

E2.2.1. Contraband, including controlled substances (particularly narcotics and dangerous drugs), as defined in Section 812 of 21 U.S.C. (reference (i)).

E2.2.2. Explosives, ammunition, firearms, and their components.

E2.2.3. Radioactive material, etiological, or other material hazardous to personnel.

E2.2.4. Flammables.

E2.2.5. Liquids.

E2.2.6. Batteries (prohibited from air shipments by the Federal Aviation Administration or international regulations), except as coordinated with the Commander, DCS, in advance.

E2.2.7. Currency, military payment certificates, bonds, securities, precious metals, jewels, postage stamps, or other negotiable instruments.

Department of Defense

DIRECTIVE

NUMBER 5205.10

December 5, 2000

ASD(C3I)

SUBJECT: Department of Defense Treaty Inspection Readiness Program (DTIRP)

References: (a) DoD Directive 5205.10, "Defense Treaty Inspection Readiness Program (DTIRP)," July 29, 1996 (hereby canceled)

(b) DoD Directive 2060.1, "Implementation of, and Compliance with, Arms Control Agreements," July 31, 1992

(c) DoD Directive 5105.62, "Defense Threat Reduction Agency (DTRA)," September 30, 1998

(d) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))," February 12, 1992

(e) DoD Directive O-5205.7, "Special Access Program (SAP) Policy, " January 13, 1997

(f) DoD Instruction O-5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," July 1, 1997

1. PURPOSE

This Directive:

1.1. Supersedes reference (a) to update policy and responsibilities for the DTIRP as a DoD arms control security preparedness and outreach program in accordance with references (b) and (c).

1.2. Directs a support program to ensure the continued protection of DoD programs, operations, and activities.

1.3. Designates the Director, Defense Threat Reduction Agency (DTRA), as the DoD Executive Agent for implementation of the DTIRP and as Chair of the DTIRP Coordination Group (CG).

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

3. DEFINITION

Defense Treaty Inspection Readiness Program (DTIRP).
A DoD security preparedness and outreach program designed to provide security education and awareness concerning arms control implementation operational activities.
It provides arms control implementation advice and assistance to sites subject to on-site inspection and overflight through the use of specially trained personnel, analyses, and educational activities, utilizing expertise from established facilities and services in the Department of Defense and other Government Agencies, whenever practicable, to avoid duplication to achieve maximum efficiency and economy.

4. POLICY

It is DoD policy that:

4.1. Security countermeasures support for implementation of arms control agreements and related activities shall be integrated and coordinated within existing DoD security and counterintelligence programs to ensure a focused approach and consistent programs for the protection of national security interests.

4.2. The Heads of the DoD Components having any involvement with arms control implementation shall ensure their facilities, activities, and programs, wherever located, have cost-effective security plans, policies, and procedures that appropriately consider arms control agreements.

4.3. The DoD Component responsible for any action taken or directed under this Directive and affecting an industrial facility shall be the DoD Component that either administers or is obligated to fund a contract involving that industrial facility. Any contact with the facility involving DTIRP matters shall be coordinated with each DoD Component administering or funding a contract at that facility.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) shall:

5.1.1. Provide security policy direction, guidance, and security oversight to the DTIRP Program, in coordination with the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), consistent with DoD Directive 2060.1 (reference (b)), DoD Directive 5105.62 (reference (c)), DoD Directive 5137.1 (reference (d)), DoD Directive O-5205.7 (reference (e)), and DoD Instruction O-5205.7 (reference (f)).

5.1.2. Coordinate with the Director, DTRA, as the DoD Executive Agent for DTIRP, to ensure DTIRP activities adequately support DoD security protection requirements.

5.1.3. Ensure that the Director, Defense Intelligence Agency, shall:

5.1.3.1. Provide all source intelligence support to the DTIRP, to include research and analyses, database development analyses, and personnel to augment assistance teams, as requested by the Director, DTRA.

5.1.3.2. Provide intelligence and security countermeasures analyses, in the areas of technology transfer, open source literature, imagery assessment, and other relevant areas, as requested by the Director, DTRA.

5.1.4. Ensure that the Director, Defense Security Service, shall:

5.1.4.1. Provide assistance in arms control security matters to DoD contractor facilities, disseminate arms control security countermeasure information and, when deemed appropriate, provide personnel to augment assistance teams as requested by the Director, DTRA.

5.1.4.2. Direct the Director, Defense Security Service Academy, to develop and conduct training on arms control security countermeasures in coordination with the Special Security Countermeasures Policy Office, ODUSD(PS).

5.1.5. Ensure the Director, Defense Information Systems Agency, shall provide multidiscipline security and intelligence support to the DTIRP, in the area of communications research and analyses, and personnel to assist in assessments as requested by the Director, DTRA.

5.2. The Under Secretary of Defense for Acquisition, Technology and Logistics shall:

5.2.1. Provide DTIRP participants with treaty compliance guidance pursuant to this Directive and DoD Directive 2060.1 (reference (b)).

5.2.2. Oversee assistance in facility preparation in support of implementation and compliance with arms control agreements and request DTIRP assistance as appropriate.

5.2.3. Ensure the Director, DTRA, as Executive Agent for DTIRP, and Chair, DTIRP CG, shall:

5.2.3.1. Develop, plan, and execute the DTIRP to provide arms control treaty inspection advice and support to DoD Components and its contractor facilities responsible for protecting DoD equities subject to arms control implementation activities on an as requested basis.

5.2.3.2. Conduct outreach activities to promote arms control security awareness to include the development of arms control educational materials in coordination with the appropriate OSD Treaty Management Office; and the dissemination of outreach products.

5.2.3.3. Recruit, train, equip, and manage the activities of DTIRP assistance teams.

5.2.3.4. Conduct analyses of arms control-specific threats to determine susceptibility and vulnerability of U.S. equities.

5.2.3.5. Provide counterintelligence (CI) support to the DTIRP process, to include augmentees for assistance teams, technical training, and analyses. Director, DTRA, shall coordinate support for DTIRP CI activities with the DoD Components.

5.2.3.6. With USD(AT&L) approval, in coordination with the Office of the Assistant Secretary of Defense for Strategy and Threat Reduction (OASD(S&TR)), provide advice and assistance on arms control security planning to non-Defense Agencies and industrial facilities, when requested and when authorized, subject to reimbursement, as appropriate.

5.2.3.7. Coordinate with the Department of Defense Security Service Academy or other training organizations, as appropriate, to develop and execute a comprehensive training program on arms control agreement issues and provide necessary resources as required, to include both industrial and Government security matters.

5.2.3.8. Coordinate, within the CG, the formulation of DTIRP requirements documents, advice on security risks associated with arms control inspection activities, software development, analyses, training and outreach

activities.

5.2.3.9. Invite the DoD Components and, in consultation with OUSD(AT&L), invite other U.S. Government Agencies having any involvement with arms control to provide representatives to the CG and convene CG meetings as required.

5.2.3.10. Develop DTIRP budget requirements and execute the budget in support of the Executive Agent mission.

5.2.3.11. Take the lead for DTIRP Public Affairs (PA) activities, to include PA planning, guidance, and fact sheets in coordination with the Office of the Assistant Secretary of Defense for Public Affairs.

5.2.3.12. Provide updates not less frequently than quarterly reviews to the Director of Security, OASD(C3I).

5.2.3.13. Provide general assistance to the DTIRP for arms control treaty verification research, development, test and engineering, and nuclear matters.

5.2.3.14. Coordinate with the Director, Special Security Countermeasures Policy Office (SSCPO), ODUSD(PS), to ensure DTIRP contacts with non-DoD personnel and foreign nationals seeking any form of arms control security education and awareness, advice, or assistance does not compromise U.S. Government positions being negotiated.

5.3. The Under Secretary of Defense for Policy shall:

5.3.1. Provide DTIRP participants with information on DoD policies and U.S. Government positions for international negotiations on arms control implementation and/or compliance issues.

5.3.2. Ensure ODUSD(PS) SSCPO provides security countermeasures policy guidance and security oversight to the Heads of DoD Components, their respective Special Access Program (SAP) Central Offices, and the OSD SAP Oversight Committee, to ensure DTIRP assistance adequately supports DoD SAPs, when required, in accordance with DoD Directive O-5205.7 (reference (e)) and DoD Instruction O-5205.11 (reference (f)).

5.4. The Chairman of the Joint Chiefs of Staff shall:

5.4.1. Provide military advice and assistance to Director, DTRA, in accordance with DoD Directive 2060.1 (reference (b)), in implementing this Directive.

5.4.2. Provide guidance for support to the Combatant Commands and coordinate on their requests for DTIRP support.

5.5. The Heads of the DoD Components shall:

5.5.1. Provide guidance for support to its Component commands, and coordinate and approve requests for DTIRP support.

5.5.2. Provide personnel to augment assistance teams, as requested by the Director, DTRA.

5.5.3. Coordinate counterintelligence and security countermeasures analyses and support for its Combatant Commands with Director, DTRA.

5.6. The Director, National Security Agency, shall provide Information Systems Security and Operations Security (INFOSEC/OPSEC) to the DTIRP, to include research and analyses and augmentees for assistance teams, as requested by the Director, DTRA.

6. EFFECTIVE DATE

This Directive is effective immediately.

SORT: **5210**.02
DOCI: **DODD 5210**.2
DATE: 19780112
TITL: **DODD 5210**.2 Access to and Dissemination of Restricted Data, January 12, 1978, USD(P), thru Ch 2, April 3, 1981 thru ch 3 November 16, 1994

Refs:(a) DoD Directive **5210**.2, "Access to and Dissemination of Restricted Data," October i8, 1968 (hereby canceled)
(b) Atomic Energy Act of 1954, as amended (Public Law 83-703)
(c) Energy Reorganization Act of 1974 (Public Law 93438)
(d) through (h), See enclosure 1

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policies and procedures governing access to and dissemination of Restricted Data by the Department of Defense. It implements reference (b) as modified by references (c) and (d). Reference (a) is hereby canceled and superseded.

B. APPLICABILITY AND SCOPE

The provisions of this Directive apply to the Office of the Secretary of Defense, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies, hereafter referred to as DoD Components.

C. DEFINITIONS

For the purposes of this Directive, definitions in enclosure 2 apply.

D. AGREEMENTS

1. In implementation of section 143 (enclosure 3) of reference (b), the Secretary of Defense notified the Atomic Energy Commission (AEC) that the established personnel and other security procedures of the Department of Defense and its agencies (DoD Regulation 52OO.1-R (reference (f)), DoD Regulation 5200.2-R (reference (g)), and DoD Regulation 52IO.22-R reference (h))) were adequate and in reasonable conformity with the standards established by the Commission. Subsequent to the enactment of the Energy Reorganization Act of 1974 (P.L. 93-438) (reference (c)) and the Department of Energy Organization Act (P.L. 95-91) (reference (1)), this notification has been reaffirmed to the successor agencies of AEC. In addition, the security procedures agreed to over the years by DoD and AEC and its successor agencies have remained in effect.

2. The Department of Defense will assume responsibility for the safeguarding of Restricted Data in its custody and control further dissemination to DoD employees and its contractors.

3. The Department of Defense will assume responsibility for assuring that those persons who sign certifications, as set forth in E.1.b.(1), are, in fact, authorized to sign them.

4. For personnel of other Federal agencies who have a need-to-know in performance of their official duties, the Department of Defense agrees to accept Department of Energy (DOE) and Nuclear Regulatory Commission (NRC) clearances for access to classified information (including Restricted Data), on the following equivalent basis:

DOE and NRC Clearances DoD Clearances

"L" (For NRC employees, consultants, and contractor SECRET personnel valid for access up to and including SECRET National Security information and Restricted Data at the CONFIDENTIAL level only)

"L" (For DOE contractor personnel only, valid for SECRET access up to and including SECRET National Security information and Restricted Data at the CONFIDENTIAL level only) ("L" clearances are not granted to internal DOE personnel)

"Q" SECRET

"Q" (With specific authority for TOP SECRET access) TOP SECRET

DoD contractor granted CONFIDENTIAL clearances are not valid for access to Restricted Data.

5. Subsequent to implementation by the National Aeronautics and Space Administration (NASA) of section 304(b) of the National Aeronautics and Space Act of 1958 (P.L. 85-568) (reference (e)), the Department of Defense and NASA have agreed that exchanges of Restricted Data related to aeronautical and space activities between personnel of the two agencies and their contractors shall be controlled and safeguarded in the same manner and under the same rules as other classified information.

E. POLICIES AND PROCEDURES

1. Access

a. Within and between DoD Components, to include contractor activities, access to Restricted Data information will be governed by the same procedures and criteria as govern the access to other classified information:

(1) Require access in performance of official duties.

(2) Have a valid DoD security clearance at a level commensurate with the information concerned.

b. Requests for access to Restricted Data in the possession of DOE or other Federal agencies designated by DOE, other than DoD and NASA, will be made utilizing DOE Form 277, "Request for Visit or Access Approval.

(1) The Secretary of Defense; the Deputy Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; the Under Secretaries of Defense; the Chairman, Military Liaison Committee (DOE-DoD); the Directors of the Defense Agencies; and their designees, are authorized to certify the need of DoD personnel, under their jurisdiction, to have access to Restricted Data in the possession of DOE and other Federal agencies designated by DOE. These officials shall forward their lists of designees to the Chairman, Military Liaison Committee, who shall transmit a composite list to DOE and to the Deputy Under Secretary of Defense for Policy Review for incorporation into enclosure 5 to this Directive. Strict adherence to "need-to-know" principles will be followed. For Navy and Air Force, the authority to certify for Restricted Data access shall not be designated below the level of the authority granting the security clearance. For Army, the authority to certify for Restricted Data access shall not be designated below Brigade level or equivalent. For contractor employees, the need for accessto Restricted Data will, in all cases, be certified by a Government Contracting Officer.

(2) Those persons listed in E.1.b.(1), or their designees, shall submit requests for access to Restricted Data directly to DOE, Director of Safeguards and Security, Washington, D. C. 20545. Requests should be forwarded through established security channels.

(3) DoD requests for access to Restricted Data, in the possession of Federal agencies other than the Department of Defense, pertaining to the Army Research Reactor Program and the Navy Research Reactor Program shall be submitted to the U.S. Nuclear Regulatory Commission, Division of Security, Washington, D. C. 20555.

(4) DoD requests for access to Restricted Data pertaining to weapons programs shall be submitted directly to the Managers of the Albuquerque or San Francisco DOE Operations Offices (or to those officials designated by these Managers), provided:

(a) The requesting activity is performing work with or for DOE or its contractors under the jurisdiction of the Albuquerque or San Francisco Operations Offices pursuant to a formal written agreement; or

(b) The requesting activity has been specifically authorized to make requests directly to DOE Managers of Operations for specific areas of mutual interest within the weapons programs.

(5) In situations other than specified in E.1.b.(3) and (4), DoD requests for access to Restricted Data in the custody of DOE personnel shall be submitted to the DOE Headquarters Division having responsibility for the subject matter involved.

(6) When it is necessary for a DoD activity to establish authority for requesting access directly from DOE Managers of Operations, a request for such authority shall be submitted to the DOE Headquarters Division responsible for the program to which access is required.

(7) DOE has authorized its personnel to accept oral requests in emergencies. In those instances, all of the information required in DOE Form 277 shall be provided. Thereafter, an appropriate written confirmation shall be forwarded. Personnel authorized to approve requests for access to or release of Restricted Data shall make determinations of emergency situations or conditions.

(8) If an individual requires repeated access to the same type of information or continuing visits to a facility, under the cognizance of the same approving authority, the request shall so specify.Local arrangements for continuing access may be made for a specified period not to exceed 1 year. Access by members of the Armed Forces may be arranged for the specified period of the assignment for which access was originally approved.

2. Dissemination

a. DoD personnel may disseminate Restricted Data information only under the following guidelines:

(1) Within and between DoD Components, to include DoD contractors, dissemination of Restricted Data information will be governed by the same procedures and criteria as govern the dissemination of other classified information.

(2) Dissemination of Restricted Data information may be made to properly cleared DOE personnel arid to DOE-cleared personnel of other Federal agencies.

(3) Dissemination of Restricted Data information pertaining only to nuclear research reactors or nuclear electric power generating reactors may be made to NRC personnel. Restricted Data not related to these reactors may be released to NRC personnel only through DOE.

(4) Dissemination of Restricted Data information other than that pertaining to aeronautical and space activities may be released to NASA personnel only through DOE.

(5) In all above cases, dissemination of Restricted Data information will be made only after the holder of the information has verified:

(a) The identification of the prospective recipient.

(b) The validity of the prospective recipient's clearance.

(c) The "need-to-know" of the prospective recipient in connection with official duties.

b. Dissemination of Restricted Data and Formerly Restricted Data to any nation or regional defense organization or to a representative thereof, is prohibited except in accordance with agreements for cooperation, entered into pursuant to section 123 (enclosure 4) of the Atomic Energy Act of 1954, as amended (reference (b)).

c. Except as provided in E.2.b., Formerly Restricted Data will be treated and disseminated in the manner prescribed for classified information in DoD Regulation 5200.l-R (reference (f)).

F. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (GNWDI)

l. Access to and dissemination of CNWDI, as defined in enclosure 2, is of particular concern to the Department of Defense. Because of the extreme sensitivity of this type of information, access must be limited to the absolute minimum number of persons who need it to accomplish their assigned responsibilities. To meet this objective, the following special procedures for controlling CNWDI information have been established.

a. Clearances and Need-to-Know

(l) As a minimum, the required security clearances for personnel eligible for access to CNWDI shall be:

(a) Final TOP SECRET or SECRET (as appropriate), or

(b) DOE "Q" for non-DoD personnel.

(2) U.S. citizenship is required, except in rare instances when an immigrant alien may possess unique or very unusual talent or skill that is essential to the U.S. Government and not possessed to a comparable degree by an available U.S. citizen. In such exceptional cases, an affirmative determination shall be made that it is in the overall best interests of the United States to grant CNWDI access to an immigrant alien. Such a determination shall be made by the Secretary of Defense or his designee, based upon the recommendation of the Head of the responsible DoD Component.

(3) Written or oral communication of CNWDI shall be strictly limited to those personnel who have a "need-to-know." Management personnel at all levels shall not automatically approve requests for access to CNWDI, but shall insist upon full justification and shall reject any requests that are not completely justified. The Head of each DoD Component and management personnel at all levels are assigned a special responsibility to insure that this "need-to-know" principle is strictly enforced.

b. Briefings. Personnel having a need for access to CNWDI shall be briefeon its sensitivity. Briefing and access authorizations will be recorded inappropriate security records. Records of CNWDI briefings and access authorizations will be maintained in a manner that would facilitate verification.

c. Marking. Documents or other media as defined in DoD Regulation 520O.l-(reference (f)), which contain CNWDI and are generated after July 1, 1978, shall be clearly marked, "Critical Nuclear Weapon Design Information - DoD Directive **5210**.2 applies." Similar documents published before July 1, 1978, and which are in working files, will be similarly marked when they are withdrawn from files. In addition, paragraphs of documents generated after July 1, 1978, which contain CNWDI, will be so marked. Example: (S-RD)(N). An (N) following the classification denotes that the classified material is additionally identified as CNWDI.

2. Within and between DoD Components, to include DoD contractors, except for the special requirements enumerated above, access to CNWDI will be controlled in the same manner as other classified information.

G. EFFECTIVE DATE

This Directive is effective immediately.

Deputy Secretary of Defense

Enclosures - 5 l. References, Continued 2. Definitions 3. Excerpt from Section 143, Atomic Energy Act of 1954, as amended 4. Excerpt from Section 123, Atomic Energy Act of 1954, as amended 5. List of Certifying Officials

REFERENCES, continued

(d) Public Law 95-91, "Department of Energy Organization Act"
(e) Public Law 85-568, "National Aeronautics and Space Administration Act of 1958"
(f) DoD 5200.l-R, "Information Security Program Regulation,"December 1978, authorized by DoD Directive 5200.1, November 29, 1978
(g) DoD 5200.2-R, " DoD Personnel Security Program Regulation," December 20, 1979 authorized by DoD Directive 5200.2, December 20, 1979
(h) DoD 5220.22-R, "Department of Defense Industrial Security Regulation," April 1975, authorized by DoD Directive 5220.22, December 1, 1976

DEFINITIONS

A. Classified Information. Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

3. Critical Nuclear Weapon Design Information (GNWI). That TOP SECRET Restricted Data or SECRET Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among theseexcluded items are the components which DoD personnel set, maintain, operate, test, or replace.

C. Department of Defense (DoD) Personnel. Military personnel in the Armed Forces, including members of the Reserve Forces and Federally recognized members of the National Guard; employees of a DoD Component, including consultants, full-time and temporary part-time employees and personnel paid from nonappropriated funds; and contractors, prospective contractors, and contractor employees of a DoD Component. (See also DoD Regulation 520O.22-R (reference (h)).)

D. DoD Security Clearance. A clearance granted by a DoD Component pursuantto the provisions of DoD Regulation 5200.2-R and DoD Regulation 520O.22-R (references (g) and (h)). (A contractor-granted CONFIDENTIAL security clearance is not valid for access to Restricted Data.)

E. Department of Energy (DOE) Personnel. DOE employees, DOE contractors and their employees, and Federal Executive Branch component personnel assigned to DOE for duty (e.g., DoD, State Department, National Aeronautics and Space Administration (NASA), etc.).

F. DOE Security Clearance. A clearance granted by DOE pursuant to provisions of the Atomic Energy Act of 1954, as amended (P.L. 83-703), the Energy Reorganization Act of 1974 (P.L. 93-438), and the Department of Energy Organization Act (P.L. 95-91) (references (b), (c), and (d)).

G. Formerly Restricted Data. Data removed from the Restricted Data category upon determination jointly by DOE and the Department of Defense that such data relates primarily to the military utilization of atomic weapons and that such data can be adequately safeguarded as classified information. Such information is, however, treated the same as Restricted Data for purposes of foreign dissemination. (See E.2.b., basic Directive.)

H. NASA Personnel. Any officer, employee, member of an advisory committee,contractor, subcontractor, or officer or employee of a contractor or subcontractor, of the NASA, and Federal Executive Branch component personnel assigned to NASA for duty (e.g., DoD, State Department, DOE, etc.).

I. NASA Security Clearance. A clearance granted by the NASA, pursuant to regulations issued by NASA.

J. Nuclear Regulatory Commission (NRC) Personnel. NRC employees, NRC contractors and their employees, and Federal Executive Branch component personnel assigned to NRC for duty (e.g., DOD, State Department, NASA, etc.).

K. NRC Security Clearance. A clearance granted by the NRC, pursuant to regulations issued by NRC.

L. Restricted Data. All data (information) concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in production of energy. The term does not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Atomic Energy Act of 1954, as amended (reference (b)). (Also see"Formerly Restricted Data.")

Atomic Energy Act of 1954, Section 143, as Amended (42 U.S.C. 2163)

Section 143. Department of Defense Participation. -- The Commission may authorize any of its employees, or employees of any contractor, prospective contractor, licensee or prospective licensee of the Commission or any other person authorized access to Restricted Data by the Commission under subsections 145b and 145c to permit any employee of an agency of the Department of Defense or of its contractors, or any meinber of the Armed Forces to have access to Restricted Data required in the performance of his duties and so certified by the head of the appropriate agency of the Department of Defense or his designee: Provided, however, That the head of the appropriate agency of the Department of Defense or his designee has determined, in accordance with the established personnel security procedures and standards of such agency, that permitting the member or employee to have access to such Restricted Data will not endanger the common defense and security: And provided further, That the Secretary of Defense finds that the established personnel and other security procedures and standards of such agency are adequate and in reasonable conformity to the standards established by the Commission under section 145.

Atomic Energy Act of 1954, Section 123, as Amended (42 U.S.C. 2163)

Section 123. Cooperation With Other Nations. -- No cooperation with any nation or regional defense organization pursuant to sections 53, 54a, 57, 64, 82, 91, 103, 104, or 144 shall be undertaken until--

a. the Commission or, in the case of those agreements for cooperation arranged pursuant to subsection 91 c. or 144 b. which are to be implemented by the Department of Defense, the Department of Defense has submitted to the President the proposed agreement for cooperation, together with its recommendations thereon, which proposed agreement shall include (1) the terms, conditions, duration, nature, and scope of the cooperation; (2) a guaranty by the cooperating party that security safeguards and standards as set forth in the agreement for cooperation will be maintained; (3) except in the case of those agreements for cooperation arranged pursuant to subsection 91 c. a guaranty by the cooperating party that any material to be transferred pursuant to such agreement will not be used for atomic weapons, or for research on or development of atomic weapons or for any other military purpose; and (4) a guaranty by the cooperating party that any material or any Restricted Data to be transferred pursuant to the agreement for cooperation will not be transferred to unauthorized persons or beyond the jurisdiction of the cooperating party, except as specified in the agreement for cooperation;

b. the President has approved and authorized the execution of the proposed agreement for cooperation, and has made a determination in writing that the performance of the proposed agreement will promote and will not constitute an unreasonable risk to the common defense and security;

c. the proposed agreement for cooperation, together with the approval and the determination of the President, has been submitted to the Joint Committee and a period of thirty days has elapsed while Congress is in session (in computing such thirty days, there shall be excluded the days on which either House is not in session because of an adjournment of more than three days): Provided, however, That the Joint Committee, after having received such agreement for cooperation, may by resolution in writing waive the conditions of all or any portion of such thirty-day period; and;

d. The proposed agreement for cooperation, together with the approval and determination of the President, if arranged pursuant to subsection 91 c., 144 b., or 144 c., or if entailing implementation of sections 53, 54a, 103, or 104 in relation to a reactor that may be capable of producing more than five thermal megawatts or special nuclear material for use in connection therewith, has been submitted to the Congress and referred to the Joint Committee and a period of sixty days has elapsed while Congress is in session (in computing such sixty days, there shall be excluded the days on which either House is not in session because of an adjournment of more than three days), but any such proposed agreement for cooperation shall not become effective if during such sixty-day period the Congress passes a concurrent resolution stating in substance that it does not favor the proposed agreement for cooperation: Provided, That prior to the elapse of the first thirty days of any such sixty-day period the Joint Committee shall submit a report to the Congress of its views and recommendations respecting the proposed agreement and an accompanying proposed concurrent resolution stating in substance that the Congress favors, or does not favor, as the case may be, the proposed agreement for cooperation. Any such concurrent resolution so reported shall become the pending business of the House in question (in the case of the Senate the time for debate shall be equally divided between the proponents and the opponents) within twenty-five days and shall be voted on within five calendar days thereafter, unless such House shall otherwise determine.

<<|IMAGE DODD0240.gif|>>

<<|IMAGE DODD0241.gif|>>

<<|IMAGE DODD0242.gif|>>

<<|IMAGE DODD0243.gif|>>

<<|IMAGE DODD0244.gif|>>

<<|IMAGE DODD0245.gif|>>

<<|IMAGE DODD0246.gif|>>

<<|IMAGE DODD0247.gif|>>

<<|IMAGE DODD0248.gif|>>

SORT: 5210.45

DOCI: DODD 5210.45

DATE: 19640509

TITL: DODD 5210.45 Personnel Security in the National Security Agency, May 9, 1964,

Refs (a) Public Law 88-290, An Act to Amend the Internal Security Act of 1950

I. PURPOSE

The purpose of this directive is to prescribe policies and procedures to implement Public Law 88-290 the objective of which Is to strengthen personnel security In the National Security Agency.

Il. PERSONNEL SECURITY STANDARD

No person shall be employed in, or detailed or assigned to, the National Security Agency, and no person shall have access to classified information of the Agency, unless his employment, detail, or assignment to the Agency, or his access to classified information of the Agency, is clearly consistent with the national security.

III. FULL FIELD INVESTIGATION

A. No person shall be finally employed In the National Security Agency until he has been the subject of a full field investigation. A person may,however, be provisionally employed before the completion of a full field investigation in his case, but he may not be given access to sensitive cryptologic information while he is so employed. His provisional employment is conditional upon the successful outcome of a full field investigation in his case.

B. No person shall be assigned or detailed to the Agency without the agreement of the Agency that its security requirements are met; each such person shall be the subject of a full field Investigation in connection with such assignment or detail unless he has a current security clearance for sensitive cryptologic information which was granted under the same or equivalent standards as are prescribed by the Agency.

C. The Director of the Agency may, in an exceptional case, temporarily waive the requirement for a full field investigation if he personally determines in writing that such action is advisable in the national interest and is clearly consistent with the national security. In such a case priority shall be given to the full field investigation. This authority of the Director, NSA, cannot be redelegated.

IV. BOARDS OF APPRAISAL

A. The Director of the Agency shall establish one or more boards of appraisal of three members each to be assigned personnel security

responsibility as set forth below. Members of a board shall be senior officials with broad experience, shall be specially trained for their duties, and shall have been the subject of a full field investigation, and have been cleared for access to classified information, in connection with their appointment

B. The Director of the Agency shall refer to a board those cases in which he determines that there is a doubt as to eligibility for access to classified information of an employee or person assigned or detailed to the Agency. The board shall appraise the loyalty and suitability of persons whose cases have been referred to it and advise the Director whether access to classified information by such persons is clearly consistent with the national security. In applying the foregoing standard,the board shall use the criteria which have been prescribed by the U. S **Intelligence** Board and Department of Defense Directive 5210.8 dated February 15, 1962.

C. Proceedings of a board shall not include notice to the individual, right to a hearing, or appeal from an adverse recommendation. A board shall submit to the Director a report and recommendation on each case referred to it. The report shall not be made available to the person. No person shall be cleared for access or continued access to Agency classified information contrary to the recommendation of a board except on the authority of the Director or, upon the referral by the Director, of the Secretary of Defense. In such a case, the Director or the Secretary shall make a determination in writing that the employment, detail, assignment or access Is In the national Interest.

D. Appraisal by a board is not required before action may be taken under Section 14 of the Act of June 27, 1944, Chapter 287, as amended (5 U.S.C. 863), Section l of the Act of August 26, 1950, Chapter 803, as amended (5 U.S.C. 22-1), or any other similar provision of law. The objective In establishing the boards(s) Is to assure further that the access of each person to classified information Is clearly consistent with the national security In consonance with the requirements and standards of the U. S. **Intelligence** Board and the Department of Defense.

V. TERMINATION OF EMPLOYMENT

A. Section 303 (a) of Public Law 88-290 authorizes the Secretary of Defense to terminate employment of any officer or employee of the National Security Agency In his discretion whenever (1) he considers such action to be in the interest of the United States, and (2) he determines that the procedures prescribed in other provisions of law that authorize the termination of employment of that officer or employee cannot be invoked consistently with the national security. The Secretary's action to terminate employment is final. The statute provides, however, that the individual whose employment has been terminated under this authority may seek or accept employment In any other Government agency provided that the Civil Service Commission determines he Is eligible for such employment.

B. When the two conditions cited above do not exist, the Director, NSA, shall, when appropriate, take action pursuant to other provisions of law, as applicable, to terminate the employment of a civilian officer or employee. The Director shall recommend to the Secretary of Defense the exercise of the authority of Section 303 (a) only when the termination of the employment of a civilian officer or employee cannot, because of

paramount national security interests, be carried out under any other provision of law.

VI. IMPLEMENTATION

Proposed implementing regulations of the National Security Agency shall be coordinated with the General Counsel of the Department of Defense prior to their publication.

VII. EFFECTIVE DATE

This directive becomes effective immediately.

Deputy Secretary of Defense

SORT: 5210.46

DOCI: DODD 5210.46

DATE: 19820128

TITL: DODD 5210.46 DoD Building Security for the National Capital Region, January 28, 1982, ASD(C)

References: (a) DoD Directive 5210.46, subject as above, January 13, 1981 (hereby canceled)
(b) DoD Directive 5100.49, "Pentagon Counterintelligence Program,11 December 3, 1965 (hereby canceled)
(c) DoD Directive 5200.8, 1Security of Military Installations and Resources," July 29, 1980
(d) Title 40, United States Code, Section 318
(e) through (i), see enclosure l

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update established policy and to assign responsibilities for DoD building security in the National Capital Region (NCR); and cancels reference (b).

B. APPLICABILITY AND SCOPE

1. The provisions of this Directive apply to those elements of the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Defense Agencies, and activities supported by the Washington Headquarters Services (WHS) (hereafter referred to as "DoD Components") occupying buildings or parts of buildings throughout the NCR that are under the authority and **control** of the General Services Administration (GSA) (hereafter referred to as GSA/DoD NCR buildings).

2. This Directive does not apply to security responsibilities for buildings located on military reservations, posts, camps, stations, installations, and activities in the NCR covered by the provisions of reference (c), unless otherwise provided by specific agreement between the Deputy Assistant Secretary of Defense (Administration) (DASD(A)) and the DoD Component concerned.

C. DEFINITIONS

1. National Capital Region. Includes the District of Columbia; Montgomery and Prince Georges Counties in Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties, and the cities of Alexandria, Fairfax, Falls Church, Manassas, and Manassas Park in Virginia. 2. Security Hours. Those designated hours when a building pass or other identification card or document, as authorized by the Director, WHS, is required for any person to gain admittance to or remain within a GSA/DoD NCR building.

D. POLICY

1. A system of building passes shall be used to **control** access to GSA/ DoD NCR buildings, except as noted in subsection B.2. Building passes shall be issued for retention and use only to persons requiring frequent and continued access to GSA/DoD NCR buildings.

2. Enclosure 2 prescribes the procedures governing the issue and use of building passes in the NCR, except as noted in subsection B.2.

3. Real property management for the buildings referred to in this Directive is vested in the GSA, under 40 U.S.C. (reference (d)). The GSA provides normal building protection, through its Federal Protective Service Division, to protect the buildings and government property therein and to provide for the safety of government occupants.

4. In space assigned to tenant agencies, the use of additional Federal Protective Service Officer and commercial contract guard services, the protection of property, and the installation, operation, and maintenance of alarms and other security devices are the responsibility of the occupying DoD Component. Such services may be provided by GSA on a reimbursable basis, provided funds are available from tenant resources. Requests for procurement of these services shall be with the full cognizance of the DoD Component's Space Management and Operations offices and shall be coordinated with and transmitted through the Area DoD Building Administrator to the Director, WHS. All requests for additional security services or security construction shall be accompanied by a detailed justification statement and citation of regulations or directives upon which the requests are based.

5. When two or more DoD Components do not agree on security policy, procedures, or counterintelligence support in GSA/DoD NCR buildings, the issue shall be referred to the Deputy Assistant Secretary of Defense (Adminstration) (DASD(A)) for final resolution.

E. RESPONSIBILITIES

1. The Director, Washington Headquarters Services (WHS), or designee, under DoD Directive 5110.4 (reference (e)), shall:

a. Provide overall administration and coordination of GSA/DoD NCR building security matters, the resolution of requests for exceptions to the provisions of this Directive, and the safety of government occupants.

b. Ensure that a pass system is prescribed and effectively implemented for GSA/DoD NCR buildings.

c. Determine design and color specifications, and manage the procurement, bulk distribution, and **control** of DoD building passes, in accordance with enclosure 2.

d. Determine when continuous security measures are to be established.

e. Monitor the security of the Pentagon building and maintain the following Pentagon security functions:

(l) Operation of the Pentagon pulping plant and incinerator, to include the scheduling of the destruction of classified waste at both sites.

(2) Liaison with DoD Components, Offices of the Public Building Service, GSA, and other U.S. agencies for the purpose of implementing the provisions contained herein.

f. Monitor counterintelligence support provided to those DoD Components occupying GSA/DoD NCR buildings that do not have an internal counterintelligence support capability or a support agreement with a DoD counterintelligence activity; coordinate, as required, the provision of support from the Military Departments and NSA, consistent with established command channels.

2. For each GSA/DoD NCR building, except the Pentagon, the Area DoD Building Administrator, designated by the Director, WHS, or his designee, shall ensure the implementation of a building security program and shall:

a. Devise and enforce security plans and procedures that are appropriate and consistent with DoD policies and regulations.

b. Issue and post security regulations, in accordance with 50 U.S.C. 797 (reference (f)).

c. Monitor the security status of the buildings or parts of buildings

occupied by DoD activities and take appropriate action to remedy unsatisfactory conditions within assigned areas of responsibility.

d. Coordinate the building security interests of the DoD tenants.

e. Maintain close liaison with building guard forces.

f. Continuously evaluate the effectiveness of the building guard forces and recommend changes when such action is warranted.

g. Provide special instructions to building guard forces, as required.

h. Regulate the introduction and use of photographic equipment in and around assigned buildings.

i. Monitor the execution of building admittance procedures to include the establishment of security hours.

j. In leased space, maintain liaison with appropriate law enforcement agencies for emergency support.

k. Ensure that sufficient arrangements for disposal and destruction of classified waste for DoD tenant agencies are made.

3. Heads of DoD Components assigned space within a GSA/DoD NCR building shall:

a. Safeguard national defense information and material as required by DoD 5200.1-R (reference (g)).

b. Issue additional security regulations to implement this Directive.

c. Forward reports on counterintelligence activities in GSA/DoD NCR buildings that involve any significant degradation of security, to the Director, WHS, or designee, for possible dissemination to DoD Components concerned. These reports are exempt from formal approval and licensing pursuant to subsection VII. G. of enclosure 3 to DoD Directive 5000.19 (reference (h)).

4. Heads of DoD Components issuing building passes shall maintain appropriate records that ensure strict accountability for all passes issued, lost, turned in, expired, or destroyed. All passes no longer required shall be collected and returned to point of issue for destruction.

F. EXCEPTIONS

Exceptions to the procedures set forth in enclosure 2 for admittance of visitors to GSA/DoD NCR buildings (except the Pentagon) may be prescribed by individual Area Building Administrators in order to accommodate special security and access requirements in buildings under their jurisdiction. Such exceptions shall be reviewed and approved by the Director, Physical Security Division, WHS, who shall also review and approve exceptions affecting the Pentagon.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Assistant Secretary of Defense (Comptroller) within 120 days.

Frank C. Callucci
Deputy Secretary of Defense

Enclosures - 2
1. References
2. DoD Building Passes
National Capital Region

REFERENCES, continued

(e) DoD Directive 5110.4, "Washington Headquarters Services," October 1, 1977

(f) Title 50, United States Code, Section 797 (g) DoD 5200.l-R, "Information Security Program Regulation," October 1980 authorized by DoD Directive 5200.1, November 29, 1978
(h) DoD Directive 5000.19, "Policies for the Management and **Control** of Information Requirements," March 12, 1976
(i) DoD 52O0.2-R, "DoD Personnel Security Program," December 20, 1979, authorized by DoD Directive 5200.2, December 20, 1979
(j) Executive Order 12036, "National Security Information," June 28, 1978 (Section 1-1104)

DoD BUILDING PASSES
NATIONAL CAPITAL REGION

A. PURPOSE

This enclosure prescribes requirements for the issuance and use of standard building passes during security hours by all persons requiring admittance to GSA/DoD NCR building that are subject to this Directive.

B. PROCEDURES

1. DoD building passes shall be issued only to U.S. nationals, immigrant aliens, and foreign exchange officers. Passes issued to foreign exchange officers shall not exceed 12 months' duration and must be requested only by the respective Army, Navy, Air Force, or Defense Intelligence Agency Foreign Liaison Office.

2. Permanent building passes shall be issued to all regularly employed DoD occupants (civilian and military) of GSA/DoD NCR buildings. Permanent passes may also be issued to other authorized persons who require continuous access to such buildings. Persons requiring access on an infrequent basis (less than 3 times per week) are not eligible for a permanent pass, but may be issued the proper temporary pass for one entry or for a specific period.

3. Normally, the expiration date on permanent passes for permanent DoD employees will be 4 years. The expiration date on permanent passes for temporary DoD employees will be the last day of the month in which the appointment expires. Employees of DoD nonappropriated fund activities and Pentagon concessionaires may be issued permanent passes of 4 years validity. Permanent passes for contractors and other authorized visitors Bill be valid for the term of the contract or not to exceed 12 months.

4. Except in the Pentagon where the wearing of an authorized building pass is mandatory from 1800 hours to 0700 hours weekdays and all day Saturdays, Sundays, and holidays, each person, civilian and military, shall show, during designated security hours, his or her DoD building pass when entering and departing a GSA/DoD NCR building, and may wear the pass in a conspicuous place on the outer clothing while in the building. If the pass is not displayed, civilians and military members must immediately show proper identification to building security force members when challenged. The Director, WHS, or his designee, may, when warranted by particular security considerations, give published notification that the display of building passes on outer clothing is mandatory in designated GSA/DoD NCR buildings during the hours and for the period specified in the notice. However, the following officials are not required to display building passes, except as requested by Federal Protective Service officers and guards uncertain of their identity:

a. Secretary of Defense
b. Deputy Secretary of Defense
c. Under Secretaries of Defense
d. Secretary of the Army
e. Secretary of the Navy
f. Secretary of the Air Force
g. Chairman, Joint Chiefs of Staff
h. Chief of Staff, Army
i. Chief of Naval Operations
j. Chief of Staff, Air Force
k. Commandant, Marine Corps
l. Assistant Secretaries of Defense
m. General Counsel of the Department of Defense
n. Assistants to the Secretary of Defense
o. Under and Assistant Secretaries of the Military Departments
p. Vice Chief of Staff, Army

q. Vice Chief of Naval Operations
r. Vice Chief of Staff, Air Force
s. Assistant Commandant, Marine Corps

5. Passes issued for access to GSA/DoD NCR buildings do not authorize access to specially designated restricted or security areas within such buildings. Admittance to these areas shall be in accordance with the pass requirements and procedures prescribed for those areas by the head of the DoD Component concerned.

6. A favorable Entrance National Agency Check (ENTNAC), National Agency Check (NAC), NAG with Written Inquiries (NACI), or a Background Investigation as prescribed in DoD~5200.2-R (reference (i)), is required for each person issued a permanent DoD building pass, except that permanent building passes may be issued, pending completion of the NAG, to permanent full-time appropriated-fund employees and permanently assigned military personnel in organizations located in GSA/DoD NCR buildings. A temporary pass may be issued, pending completion of the NAC, to permanent full-time appropriated-fund employees and permanently assigned military personnel in organizations located in GSA/DoD NCR buildings. A temporary pass may be issued to other authorized personnel, provided an ENTNAC, NAC, NACI, or BI is initiated immediately. If it is determined that the results of the ENTNAC, NAG, BI, or NACI are unfavorable, the temporary or permanent pass issued pending completion of the appropriate security checks or investigations shall be withdrawn immediately by the issuing DoD Component. A permanent pass may be issued to immigrant aliens only upon completion of a favorable BI.

7. Passes shall be designed to be reasonably tamperproof. Each pass shall be individually numbered in its initial manufacture and shall be accounted for at all stages of handling.

8. The issuance of passes permitting access to more than one building shall be justified on an "as required" basis.

9. Upon routine transfer of a passholder from one DoD Component to another within the NCR, retention of a valid pass is authorized. Accountability shall be assumed by the gaining Component. The losing Component shall notify the building pass office of the passholder's new organization.

10. The DoD Component requesting a permanent building pass for an individual shall ensure that the person has a definite need for access to a GSA/DoD NCR building or buildings and verify that the individual has had a favorable ENTNAC, NAC, NACI, or BI. The requesting Component shall monitor the continuing requirement for the passholder to retain his oil her pass and deliver collected passes to point of issue.

11. Each passholder shall exercise every precaution to preclude loss of his or her pass; however, if a pass is lost, the loss shall be reported immediately to proper authority. Appropriate administrative action shall be taken by the responsible DoD Component in instances involving negligent loss, willful destruction or alteration, misuse of any pass, or failure to report loss immediately.

C. TYPES OF BUILDING PASSES

1. DoD Building Pass (DD Form 1466). A permanent pass for personnel who regularly work in or require frequent access to GSA/DoD NCR buildings during security hours. This pass shall indicate on the face thereof that it is for use in "All DoD" buildings or the specific building for which it is valid.

2. Temporary DoD Building Pass (DD Form 1469). A pass for use during security hours in GSA/DoD NCR buildings for persons whose presence therein is required for a limited period of time, or for individuals awaiting completion of an ENTNAC, NAC, NACI, or BI. This pass shall be issued only for such period of time as is necessary, up to a maximum of 120 days. Request for DoD Temporary Building Pass (DD Form 1471) shall be submitted by the requesting DoD Component to the issuing authority.

3. Visitor Passes. There are two types of visitor passes, escort and nonescort, which shall be used for the conduct of DoD business only and shall identify the specific building in which the pass is valid. Visitor passes shall be issued for one entry and shall normally be returned to the

point of the entry when the visitor departs from the building. A record of issuance shall be maintained at the point of entry. All visitors shall be the responsibility of the DoD Component requesting admittance.

a. Escort Required Visitor DoD Building Pass (DD Form 1470-1). A pass for visitors having infrequent business with specific individuals or offices within a GSA/DoD NCR building. Such visitors shall be issued this pass during security hours and shall be escorted at all times by properly identified escorts provided by the office to be visited.

b. Nonescort Visitor DoD Building Pass (DD Form 1470)

(1) Designated persons having infrequent business with specific individuals or offices may be issued nonescort-type passes upon receipt of an official written request from the requesting DoD Component.

(2) This pass may also be used to meet special requirements in a specific GSA/DoD NCR building when authorized by the proper DoD official responsible for building administration.

D. PRESS PASSES

Press passes are issued by the Director, WHS, or designee, through prior agreement and coordination with officials in the Office of the Assistant Secretary of Defense (Public Affairs).

Department of Defense Instruction 5210.52

Security Classification of Airborne Sensor Imagery and Imaging Systems

18 May 1989

Department of Defense
INSTRUCTION

May 18, 1989
NUMBER 5210.52

ASD(C3I)

SUBJECT: Security Classification of Airborne Sensor Imagery and Imaging Systems

References: (a) DoD Instruction 5210.52, "Security Classification of Airborne Sensor Imagery," September 26, 1973 (hereby canceled)
(b) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
(c) DoD Instruction 5210.51, "Security Classification Concerning Airborne Passive Scanning Infrared Imaging Systems," September 26, 1973 (hereby canceled)
(d) DoD Instruction 5210.57, "Security Classification Concerning Airborne Radar Imaging System," September 26, 1973 (hereby canceled)
(e) through (k), see enclosure 1

A. REISSUANCE AND PURPOSE

This Instruction:

1. Reissues reference (a) to implement revisions to reference (b).

2. Consolidates into one document references (c) and (d).

3. Updates policy, procedures, and responsibilities.

B. APPLICABILITY AND SCOPE

This Instruction:

1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments (including their National Guard and Reserve components), the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

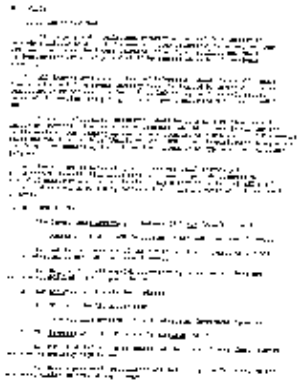
2. Will be incorporated to the extent applicable into contracts of DoD Components.

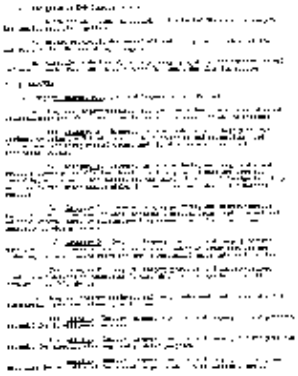
3. Applies to U.S. Government Agencies and approved non-Government users as a condition for receiving imaging systems information from DoD Components.

4. Applies to all airborne sensor imagery and imaging systems produced by or for any element of the Department of Defense.

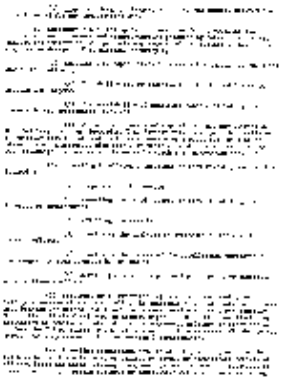
C. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

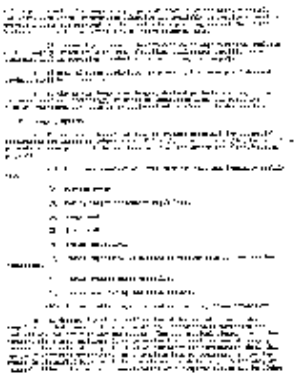




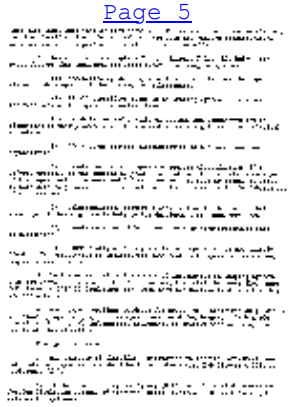
Page 3



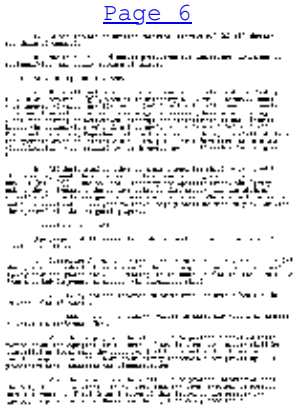
Page 4



Page 5



Page 6



Page 7

c. The ultimate classification of the inquiry shall be the highest of the classifications determined [illegible] paragraphs 6.b.(1) through 6.b.(3), above.

6. EFFECTIVE DATE AND IMPLEMENTATION

This instruction is effective immediately. Forward three copies of the [illegible] implementing documents to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) within 120 days.

Thomas P. Quinn
Principal Deputy [illegible]

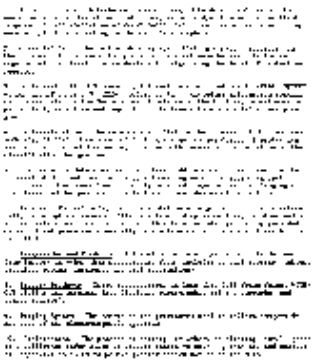
Enclosures - 6
1. References
2. Definitions
3. Classification Considerations
4. Classification Guides
5. Classification or Airborne Intelligence
6. Downgrading, Declassification, and Public Release

Page 8

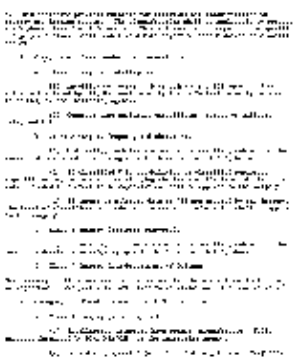
REFERENCES, continued

(e) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
(f) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984
(g) Executive Order 10104, "Defining Certain Vital Military and Naval Installations and Equipment as Requiring Protection Against the General Dissemination of Information Relative Thereto," February 1, 1950
(h) Executive Order 12356, "National Security Information," April 2, 1982
(i) DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," March 1986, authorized by DoD Directive 5200.1, June 7, 1982
(j) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984
(k) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 2, 1982

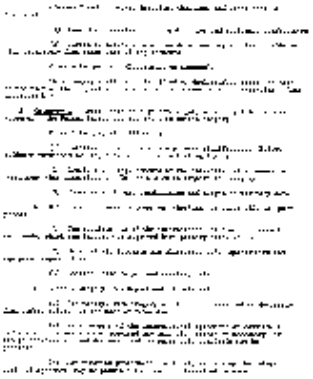
Page 9



Page 10



Page 11



Page 12

4. Category D. Foreign areas not under any national sovereignty.

a. Class 1 imagery (intelligence)

(1) Intelligence interests have primary significance. Follow guidance furnished by DIA, USD/ISA, or the initiating Agency.

(2) Consider classified U.S. capabilities and equipment capabilities.

(3) Consider also target and military data aspects.

b. Classes 2 (mapping and charting), 3 (official purposes), and 4 (non-DoD) imagery.

Treat the same as Category A., above; classes 2, 3, and 4 imagery, respectively.

5. Category E. Imagery not covered in categories A. through D., above.

Only c and 1 imagery (intelligence) shall be involved in category E. Consequently, intelligence considerations shall control classification of this imagery.

Page 13

Page 14

c. Classification of the equipment used that have been classified by the DoD activity responsible for the equipment.

d. Practical considerations based on conditions at the acquisition site may affect the classification to be applied to the imagery obtained. When possible, consider the following factors when designating the classification guidance for the plan, program, project, or operation. The requiring activity may weigh and apply them to the imagery.

(1) The availability, including capability and opportunity, of other nations to acquire the same imagery.

(2) The known or reasonably suspected availability of the same imagery to other nations, particularly those that are hostile and might use the imagery to the detriment of the United States.

(3) The means available to protect the area covered by imagery from airborne surveillance.

(4) The concealment of critical or classifiable installations, activities, or foreign features from airborne surveillance.

e. Review also DoD 5200.1-R (reference (i)). Security classification guidance developed according to this Instruction must list and clearly critical technology as provided in DoD Directive 5000.2 (reference (j))

Page 15

Page 16

(1) Flight path might reveal the extent of U.S. capabilities, activities, destination, violation of sovereign rights, international agreements, or commitments, or areas of acquisition.

(2) Imagery might reveal inadvertent violation of sovereign rights, international agreements, or commitments.

(3) Interpretation and special exploitation might reveal classified capabilities of equipment used, areas and scope of interest, certain features or otherwise identifiable and data that is not readily accessible.

3. Technical adjustment of the imagery, such as the following:

a. Rectification, to change the scale or obliquity to provide classifiable capabilities of the equipment used for means of acquisition.

b. Tracking to rectify terrain features and correct information on when the imagery was taken or other details.

c. Superimposition of data associated with the imagery, imagery would be exposed, but may be limited to areas such as digital verification and/or identification, deletion of some items as "markers" used while operating, artwork (symbols), deforming introduction of noise into the image, and maintaining grey scale to operate the image.

4. Combination of descriptive data to hide the source or means of acquisition, dilute or the purpose of, consolidate, or increase the classification of more than one, or add data acquisition to compatible existing data of lower or no security classification.

Page 17

DOWNGRADING, DECLASSIFICATION, AND PUBLIC RELEASE

a. Experienced customer users and holders of imagery who have been designated expressly by the program initiator are authorized to make imagery less sensitive or accumulative. They do this by removing the highly classified aspects or all classified aspects of the imagery using the sanitization process given in enclosure 3. Program initiators shall ensure these designations are limited to those with a sufficient degree of expertise to maintain without endangering the security of the original imagery. Other users and holders of imagery, and others with questions that this instruction may not resolve, shall consult the initiator of the plan, program, project, or operation. Initiators who are original classification authorities must advise recipients of changes in imagery classification policy, to include declassification of imagery that has not been sanitized.

b. It is essential to prevent the indefinite classification of imagery when possible. A date or event for declassification shall be determined in advance, such as: "Declassify on 1 Jan 93." "Automatically 30 days after imagery." "Declassify on Completion of the (Name) Program." "Declassify one year after cessation of hostilities," or similar language, rather than "Originating Agency's Determination Required". (See DoI 5200.1-R (reference (b)).

c. Public release of imagery is governed by enclosures 4 and 5 of this instruction and DoD Directive 5230.9 (reference (k)).

Department of Defense

DIRECTIVE

NUMBER 5210.55

December 15, 1998

(ES, OSD)

SUBJECT: Department of Defense Presidential Support Program

References: (a) DoD Directive 5210.55, "Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities," July 6, 1977 (hereby canceled)

(b) DoD Instruction 5210.87, "Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities," November 30, 1998

(c) DoD Directive 1000.17, "Detail of DoD Personnel Assigned to Duty Outside the Department of Defense," July 28, 1988

(d) through (f), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policies and assign responsibilities.

1.2. Is implemented by reference (b) prescribing the procedures for the nomination, screening, selection, approval and continued evaluation of DoD military and civilian personnel, and contractor employees assigned to, or retained in Presidential support duties.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies and the DoD Field Activities (hereafter referred to collectively as "the DoD Components") having a Presidential support mission.

2.2. Encompasses all DoD organizations and, through incorporation of its terms into contracts, contractors that assign personnel to Presidential support duties involving regular or frequent access to the President or Vice President, or to facilities that support the President or Vice President, including communications activities and modes of transportation.

2.3. Does not apply to DoD personnel or contractors whose duties involve infrequent visits to the Executive offices of the White House or other Presidential support facilities to conduct official business with the Presidential and/or Vice Presidential staffs.

2.4. Does not apply to personnel providing Presidential protection support duties or personnel assigned to other duties supporting the President on a temporary, intermittent, or seasonal basis, not to exceed an aggregate of 180 days in either a single continuous assignment or series of assignments.

2.5. Does not establish reimbursement policies or procedures. The policies for reimbursements and applicable amounts to be recouped are in DoD Directive 1000.17 (reference (c)).

2.6. Does not apply to details made pursuant to 3 U.S.C. 112 (reference (d)) or DoD Directive 1000.17 (reference (c)) to the Executive Office of the President or the agencies of the Executive Office of the President.

3. DEFINITION

3.1. Presidential Support Facilities. The temporary or permanent areas designed, intended or maintained for sole support of the President or Vice President.

4. POLICY

It is DoD policy that:

4.1. The President shall be provided with the optimum level of security and support.

4.2. Persons assigned to, or retained in Presidential support duties, shall be the best suited and best qualified for these duties, based on a determination that their assignment or retention is clearly consistent with optimum Presidential security and support.

4.3. All persons serving in Presidential support duties must be U.S. citizens.

4.4. Denial or revocation of a security clearance for access to classified information shall automatically result in disqualification for Presidential support duties.

4.5. Any DoD civilian or contractor employee not approved for, or removed from, Presidential support duties shall be afforded an opportunity to appeal this decision, unless the individual is disqualified as provided in subsection 4.4., above. Military personnel are not afforded the opportunity to appeal, unless the assignment policies of the Military Departments concerned allow for such appeals in assignment actions.

4.6. The investigative requirements and adjudicative standards for persons serving in Presidential support duties shall be in accordance with reference (c) and DoD 5200.2-R (reference (e)).

4.7. All persons assigned to Presidential support duties will be volunteers for assignment to, or work in support of, the Presidential support mission. However, when volunteers are not available for enlisted support positions, qualified enlisted non-volunteers may be nominated.

4.8. The tour of duty for all military personnel selected for assignment to Presidential support duties shall be stabilized for the maximum period allowable under the assignment policies of the Military Department concerned, with a minimum of two years from the date of assignment

to Presidential support duties. Waivers of obligated service to meet this requirement will be considered on a case-by-case basis by the Executive Secretary of the Department of Defense. This policy does not apply to Honor Guard units, Social Aides or White House NCOs assigned to the Military Departments.

5. RESPONSIBILITIES

5.1. The Executive Secretary of the Department of Defense shall be the final approval authority for assignment of individuals used in Presidential support duties and for general oversight of the implementation of this Directive. Waiver of specific requirements in this Directive may be granted only by the Executive Secretary.

5.2. The Heads of the DoD Components with a Presidential support mission shall:

5.2.1. Designate a single office to represent the DoD Component on all matters covered by this Directive at the Service secretariat or comparable Defense Agency level. Responsibilities of DoD Components under this Directive may not be delegated below this level.

5.2.2. Ensure individuals are identified for assignment to Presidential support duties, either as initial appointees or replacements, in a timely manner to permit processing of the required investigations and higher level review before assignment.

5.2.3. Ensure that replacements are assigned for individuals who complete their tours of duty in Presidential support positions unless the requirement is discontinued.

5.2.4. Ensure that the requirements of this Directive are incorporated into the contract of each contractor involved in Presidential support duties.

5.2.5. Establish procedures to evaluate the continued suitability of personnel serving in Presidential support duties and management personnel exercising supervision over contractor employees performing Presidential support duties in accordance with reference (b).

5.2.6. Report to the Executive Secretary on a periodic basis information about personnel assigned to Presidential Support Duties in accordance with DoD Instruction 5210.87 (reference (b)).

6. INFORMATION REQUIREMENTS

The reporting requirement identified in Section 5., above and further described in DoD Instruction 5210.87 (reference (b)) has been assigned Report Control Symbol DD-5D(Q)934, in accordance with DoD 8910.1-M (reference (f)).

7. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 1

1. References, continued

E1. ENCLOSURE 1

REFERENCES, continued

(d) Title 3, United States Code

(e) DoD 5200.2-R, "DoD Personnel Security Program," January 1987, authorized by DoD Directive 5200.2, May 6, 1992

(f) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 8910.1, June 11, 1993

SORT: 5210.78

DOCI: DODD 5210.78

DATE: 19910918

TITL: DODD 5210.78 Department of Defense Polygraph Institute (DoDPI), September 18, 1991, ASD(C3I)

Refs:(a) DoD Directive 5210.78, subject as above, October 17, 1986 (hereby canceled)
(b) DoD Directive 521O.48, "DoD Polygraph Program," December 24, 1984
(c) DoD 5025.1-M, "DoD Directives System Procedures," December 1990, authorized by DoD Directive 5025.1, December 23, 1988
(d) DoD 5210.48-R, "Department of Defense Polygraph Program," January 1985, authorized by reference (b)

A. REISSUANCE AND PURPOSE

This Directive:

1. Reissues reference (a) to update policy and responsibilities and clarify the DoDPI mission as an educational and research facility supporting the DoD Polygraph Program (reference (b)).

2. Designates the Secretary of the Army to provide support to the DoDPI.

3. Authorizes various DoD technical publications on psychophysiological detection of deception (PDD) and related areas by the DoDPI, subject to reference (c) and the approval of the Assistant Secretary of Defense for Command, Control, Communication, and **Intelligence** (ASD(C3I)).

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified. Commands, and the Defense Agencies(hereafter referred to collectively as "the DoD Components").

C. POLICY

1. The DoDPI is an organization of higher education and provides a DoD-certified Program of Instruction (POI) in basic and advanced PDD, conducts PDD research, and offers instruction and research advisory service to the DoD Components. The

instructors (researchers) employed by the DoDPI will maintain a high level of proficiency in technical and instructional skills and be engaged in ongoing programs of research.

2. It is the policy of the DoDPI that its POI is maintained at an optimal level of proficiency. Its courses of instruction shall be uniform and current and shall make use of the most advanced and effective PDD research technology.

3. As student billets become available, the DoDPI may support other Federal law enforcement agencies. It may also support, on a reimbursable basis, State and local law enforcement agencies.

D. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communication, and **Intelligence** shall:

a. Have authority, direction, and control of the DoDPI.

b. Serve as reviewing and final approval authority for the POI and research programs to ensure that the programs are based on DoD policy objectives.

c. Establish procedures for admission of non-Federal Agency personnel to the DoDPI.

d. Assess the DoD Components' use of advanced training courses other than those provided by the DoDPI to ensure that the courses satisfy the DoD's policies and objectives.

e. Establish and chair a DoDPI Advisory Committee consisting of the DoD Component Polygraph Program Managers. The committee shall meet at least annually to discuss, plan, and review, and otherwise advise the Director, DoDPI on the POI, ongoing education programs, training and research programs, and other matters pertinent to the effective operation of the DoDPI. The Director of the DoDPI shall establish the agenda after consulting with the ASD(C3I) and the DoD Component Polygraph Program Managers. Non-DoD Federal Agencies using the DoDPI may provide recommendations on oversight and POI matters to the ASD(C3I), and heads of non-DoD Federal polygraph programs may serve as associate members of the Advisory Committee at the discretion of the committee Chair.

f. The Heads of the DoD Components with polygraph programs shall:

(1) Make available to the DoDPI pertinent PDD-related materials, records, case files, and quality control procedures as required by the DoDPI to accomplish its mission.

(2) Use the DoDPI exclusively for basic PDD education and training, and use the DoDPI as necessary for advanced PDD education and training.

(3) Sponsor and support PDD research at the DoDPI when required.

(4) Advise the ASD(C3I) of courses used for advanced PDD training other

than those provided by the DoDPI.

2. The Secretary of the Army shall:

a. Provide and maintain facilities for operating the DoDPI.

b. Provide administrative, logistical, and special funding support.

c. Include the annual budget of the DoDPI, as developed in consultation with the ASD(C3I), as a separate line item in the Department of the Army Budget and Financial Plan.

d. Provide personnel for practical exercises and for research purposes, to include paid examinees from local universities and communities as clinical and research requirements dictate.

E. EFFECTIVE DATE

This Directive is effective immediately.

Donald J. Atwood Deputy Secretary of Defense

SORT: **5210**.79
DOCI: **DODD 5210**.79
DATE: 19920709
TITL: **DODD 5210**.79 Defense Personnel Security Research Center (PERSEREC), July 9, 1992, ASD(C3I)

Refs:(a) DoD Directive **5210**.79, "Defense Personnel Security Research and Education Center," May 31, 1989 (hereby canceled)
(b) Title 10, United States Code
(c) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982

A. REISSUANCE AND PURPOSE

This Directive:

1. Reissues reference (a) to update the PERSEREC, established under reference (b).

2. Assigns direction, authority, and control over the PERSEREC to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)).

3. Designates the Secretary of the Navy to provide support to PERSEREC.

4. Prescribes the policy for and responsibilities of the PERSEREC.

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

C. POLICY

It is DoD policy that the PERSEREC:

1. Shall be the DoD personnel security research center for the Department of Defense, operating under the guidance and authority of the ASD(C3I).

2. Shall perform personnel security research and analysis for the DoD Components and members of the Intelligence Community, as appropriate, and disseminate results of that research.

3. Shall devote its research and analytical resources to evaluating and improving personnel security procedures, programs, and policies.

4. Shall provide advice and assistance to the DoD Components and the Intelligence Community on selected personnel security subjects upon request.

5. Shall encourage Government and non-Government researchers to enter into joint personnel security research projects that have Government-wide applications, thereby stimulating research and reducing duplication of effort.

6. Shall ensure that individual records are maintained and used in accordance with the Department of Defense Privacy Program requirements (DoD Directive 5400.11, reference (c)).

7. Shall arrange for contractual agreements using normal contracting

procedures to meet the PERSEREC professional and administrative requirements. The PERSEREC may accept funding from other DoD Components, as well as Executive Branch Agencies, for the conduct of relevant personnel security research, subject to prior coordination with the ASD(C3I).

8. Shall maintain liaison with other DoD Components, industry, professional associations, academia, Government organizations (Federal, State, and local), and other Federal and international agencies for the exchange of information in the field of assigned responsibility; and render assistance, as appropriate, within the limits of established policy and procedures.

D. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence shall:

a. Have authority, direction, and control of the PERSEREC.

b. Promulgate a memorandum of understanding with the Secretary of the Navy that will provide administrative and logistics support required to ensure the continued effective operation of the PERSEREC.

c. Ensure that the PERSEREC is operated efficiently and that appropriate management safeguards are in place to prevent fraud, waste, and abuse.

d. Approve the PERSEREC annual budget before its submission to the Navy.

e. Convene a personnel security research advisory committee that shall:

(1) Review, on a semiannual basis, the research program of the PERSEREC.

(2) Advise the Director, PERSEREC, on specific research projects.

(3) Promote collaborative initiatives, eliminate redundancies, identify neglected opportunities and problems, and ensure optimal utilization of PERSEREC resources.

(4) Promote dissemination of useful information derived from personnel security research efforts.

f. Be authorized to make exceptions to the requirements of this Directive on a case-by-case basis when is is determined that doing so furthers -the mission of the Department of Defense and is consistent with the protection of classified information from unauthorized disclosure.

2. The Secretary of the Navy shall:

a. Budget for and finance those expenses for operating the PERSEREC, including salaries of assigned civilian personnel.

b. Provide and maintain facilities essential to the effective operation of the PERSEREC.

c. Provide administrative support to the PERSEREC to include supply, contractual, computer, and employee service assistance.

d. Assist the PERSEREC in specific personnel matters, to include managing local hiring authority for civilian personnel.

3. The Heads of the DoD Components shall:

a. Cooperate with and assist the Director of the PERSEREC by providing assistance to complete assigned research tasks.

b. Subject to internal policies on release of personnel security and criminal investigative records, make available those records and information needed by the PERSEREC to carry out the functions assigned by this Directive.

4. The Assistant Secretary of Defense (Force Management and Personnel) shall ensure that sufficient computer programming and analysis resources are made available at the Defense Manpower Data Center to support PERSEREC requirements.

E. EFFECTIVE DATE

This Directive is effective immediately.

Donald J. Atwood Deputy Secretary of Defense

SORT: **5215**.01
DOCI: **DODD 5215**.1
DATE: 19821025
TITL: **DODD 5215**.1 Computer Security Evaluation Center, October 25, 1982 thru ch 1 November 16, 1994

Ref: (a) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972
(b) DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by reference (a)
(c) QMB Circular No. A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," July 27, 1978
(d) through (m), see enclosure 1

A. PURPOSE

This Directive establishes the DoD Computer Security Evaluation Center (CSEC), provides policy, and assigns responsibilities for the technical evaluation of computer system and network security, and related technical research.

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. Its provisions govern the conduct of trusted computer system evaluation and technical research activities within the Department of Defense in support of overall computer system security evaluation and approval responsibilities assigned to the DoD Components under references (a), (b), (c), DoD Directives 5220.22, and 5400.11 (references (d) and (e)).

C. DEFINITIONS

1. Sensitive/Classified Information. Sensitive information as defined in reference (c), and classified information as defined in DoD 520O.1-R (reference (f)).

2. A Trusted Computer System. Employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

3. Generic Computer Security Research and Development. Has potential application over a very broad, generalized basis, and includes experimental exploration and development of feasible and potentially useful technology, responsive to a broad class of computer security needs.

D. POLICY

1. It is DoD policy to encourage the easy availability of trusted computer systems. The establishment of the DoD CSEC, the consolidation of generic computer security research and development (R&D), the evaluation of computer security systems and the establishment of an Evaluated Products List (EPL) are designed to further this objective.

2. The DoD Consolidated Computer Security Program (CCSP) shall include resources for the operation of the CSEC and for generic computer security R&D activities in support of DoD Components. The DoD Components are responsible for DoD Component security research, development, test, and evaluation (RDT&E) efforts and application-dependent research and development for specific DoD Component systems.

3. The activities and products of the CSEC, including technical advice and support, shall complement the established responsibilities of DoD Components relating to the overall policy, security evaluation, and approval of computer systems as prescribed in DoD Directive 5200.28, DoD 5200.28-M, OMB Circular A-71, Directives 5220.22 and 5400.11 (references (a), (b), (c), (d), and (e)), for the processing, use, and production of sensitive and classified information.

4. The EPL is not intended to replace prescribed procurement practices in the acquisition of computers and computer services. The CSEC and EPL are established to assist procuring activities in evaluating available products; computer products or services will not be rejected on the basis that the product or service is not on an EPL.

E. PROCEDURES

Procedures for consolidated technical research are at enclosure 2.

F. RESPONSIBILITIES

1. The Under Secretary of Defense for Research and Engineering (USDR&E), or his designee, shall:

a. Provide overall policy direction, guidance, and management over-sight for the CSEC in coordination with the Deputy Under Secretary of Defense (Policy) (DUSD(P)) and the Assistant Secretary of Defense (Comptroller) (ASD(C)).

b. Establish a steering committee composed of representatives of DoD Components to review center activities and recommend future directions.

c. In coordination with the Deputy Assistant Secretary of Defense (Policy)(DUSD(P)) and the Assistant Secretary of Defense (Comptroller) (ASD(C)) represent the Secretary of Defense with other government agencies, foreign governments, the North Atlantic Treaty Organization (NATO), and to the extent permitted, industry, in trusted computer system evaluation policy matters. Enter into agreements, if appropriate, consistent with National

Disclosure Policy (reference (g)), with other government agencies, foreign governments, and NATO.

d. Establish an information exchange forum on computer security matters among DoD Components.

2. The Director, National Security Agency (NSA), in cooperation with the USDR&E, shall::

a. Establish and operate the CSEC as a separate and unique entity within the NSA.

b. Program and budget for CCSP support resources under procedures prescribed for the DoD planning, programing, and budgeting processes, but excluding National Foreign Intelligence Program funds controlled by the Director of Central Intelligence (DCI) under E.O. 12333 (reference (h)).

c. Appoint a Director to manage the CSEC who shall:

(1) Establish and maintain technical standards and criteria for the evaluation of trusted computer systems that can be incorporated readily into the DoD Component life-cycle management process (DoD Directives 7920.1, 5000.29, 5000.1, 5000.2 (references (i),(k),(l),(m)). Provide assistance to the DoD Components in the application of the technical standards and criteria.

(2) Conduct evaluations of selected industry and government-developed trusted computer systems against these criteria. Request for evaluation ofgovernment-developed computer systems will be from the DoD Component responsible for the security of the system to be evaluated.

(3) Maintain and publish an EPL of the selected industry and government-developed trusted computer systems that is suitable for use by the DoD Components.

(4) Conduct and sponsor R&D for trusted computer systems, and for computer security evaluation and verification methods and techniques.

(5) Provide assistance to the DoD Components by conducting evaluations of selected DoD and DoD contractor trusted computer systems in response to requests from the DoD Component responsible for the security of the computer system to be evaluated.

(6) Serve as the focal point for technical matters concerning the use of trusted computer systems for the protection of sensitive and classified information and, in conjunction with DoD Component computer security test and evaluation activities, provide technical advice to the DoD Components.

(7) Sponsor DoD Component cooperative efforts, public seminars, and workshops for the purpose of technology transfer.

(8) Serve as the DoD principal technical point of contact on trusted computer system matters with other government agencies, industry, foreign governments, and NATO under the policy guidance of the USDR&E or designee, consistent with National Disclosure Policy (reference (g)).

(9) Develop and maintain the CCSP, in conjunction with DoD Components. (See procedures at enclosure 2).

3. Heads of DoD Components, or designees, shall:

a. Make maximum use of the standards, technical criteria, and evaluations promulgated by the CSEC in meeting their responsibilities for overall automatic data processing (ADP) system security evaluation, approval, and maintenance as set forth in DoD Directive 5200.28, DoD 5200.28-M, DoD Directives 5220.22, and 5400.11 (references (a), (b), (d), and (e)).

b. Establish overall ADP security policy for specific types of sensitive and classified information under their security cognizance, and prescribe the security procedures and constraints appropriate for the classes of trusted computer systems as defined in the EPL.

c. Designate central DoD Component focal points for interaction with the CSEC in the development of Component trusted computer systems.

d. Formulate jointly the CCSP and manage directly the execution of their respective portions of the CCSP in accordance with enclosure 2.

e. Conduct RDT&E to meet specific operational needs identified by Component requirements.

G. EFFECTIVE DATE

This Directive is effective immediately.

Frank C. Carlucci Deputy Secretary of Defense

Enclosures - 2 1. References 2. Summary of Procedures for Consolidated Technical Research

REFERENCES, continued

(d) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
(e) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
(f) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982
(g) DoD Instruction 5230.17, "Procedures and Standards for Disclosure of Military Information to Foreign Activities," August 17, 1979
(h) Executive Order 12333, "United States Intelligence Activities" December 4, 1981
(i) DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems (AIS)," October 17, 1978
(j) DoD Directive 7200.1, "Administrative Control of Appropriations," November 15, 1978
(k) DoD Directive 5000.29, "Management of Computer Resources in Major Defense Systems," April 26, 1976
(l) DoD Directive 5000.1, "Major Systems Acquisition," March 9, 1982
(m) DoD Directive 5000.2, "Major Systems Acquisition Process," March 19, 1980

PROCEDURES FOR CONSOLIDATED TECHNICAL RESEARCH

This establishes the procedures for developing the generic computer security R&D portion of the CCSP, as defined in subsection C.3. of this Directive. Portions of the CCSP relating solely to the operations of the CSEC are not included in this summary.

1. Under paragraph F.2.b of this Directive, the Director, NSA, shall issue a data call for each fiscal year to the DoD Components for the CCSP. The data call shall request identification of major tasks and milestones for that fiscal year.

2. DoD Components shall submit to NSA their proposed projects for generic computer security R&D in the format prescribed. This shall include a program-quality technical description, cost estimates, and recommendation for the execution responsibility, namely, the submitting Component, another Component, or the CSEC. The CSEC similarly shall prepare its own proposals.

3. The CSEC shall convene the technical review group (TRG) composed of an identified principal from each DoD Component with participation by the working level engineering, scientific, communications and data processing personnel of DoD Components and the CSEC. The purpose and function of this group is to review the Component submissions for redundancies, completeness, and resource requirements, and to determine initial priorities. The TRG deliberations are directed toward an understanding andagreement among all principals of the nature and scope of the proposed CCSP research and development projects.

4. The CSEC shall compile the TRG-reviewed projects and provide the DoD Components a copy of the draft program for review and comment.

5. The Director, CSEC, shall chair the program working group (PWG) which is composed of a principal from each DoD Component. The function of the PWG is to review and refine the priorities for the generic security R&D portion of the CCSP under published OSD guidance. The PWG shall recommend the generic computer security R&I) program to the Director, NSA. The CSEC shall prepare the draft consolidated computer security R&D program and provide the Components a copy for review and comment.

6. The Director, NSA, shall chair the program manager's review group (PMRG) consisting of representatives from DoD Components, including the Deputy Assistant Secretary of Defense (Communications, Command, Control, and Intelligence) and the Deputy Assistant Secretary of Defense (Research and Advanced Technology) as members, with additional observers, as appropriate. A formal briefing on the overall CCSP shall be presented to the Director and this group.

7. The Director, NSA, shall approve the CCSP after considering the changes or modifications suggested by this review group. This shall constitute thebasis for the CCSP portion of the NSA Program Objectives Memorandum (PON) submission.

8. Acting upon published guidance and based on the approved CCSP, NSA shall make the budget submission for the CCSP. The CSEC shall distribute the CCSP portion of the NSA POM submission to the DoD Components.

9. Before anticipated appropriation, the PWG shall refine further priorities, confirm execution responsibilities, and identify possible candidates in the event of program reductions. These actions shall be the basis for suballocation of funding.

10. Following receipt of obligational authority, NSA shall suballocate CCSP funds to DoD Components for their approved tasks under DoD Directive 7200.1 (reference (j)). The sub allocation process requires that each DoD Component provide to NSA by the 15th of each month a status report of commitmenace and obligations of the CCSP funds.

Department of Defense

DIRECTIVE

NUMBER 5220.6

January 2, 1992

Administrative Reissuance Incorporating Through Change 4, April 20, 1999

GC, DoD

SUBJECT: Defense Industrial Personnel Security Clearance Review Program

References: (a) DoD Directive 5220.6, subject as above, August 12, 1985 (hereby canceled)

(b) DoD 5200.2-R, "Department of Defense Personnel Security Program," January 1987, authorized by DoD Directive 5200.2, December 20, 1979

(c) Section 1001 of title 18, United States Code

(d) Section 101 et seq. of title 28, United States Code

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policy, responsibilities, and procedures of the Defense Industrial Personnel Security Clearance Review Program implementing enclosure 1.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Inspector General of the Department of Defense (IG, DoD), and the Defense Agencies (hereafter referred to collectively as "the DoD Components").

2.2. By mutual agreement, also extends to other Federal Agencies that include:

2.2.1. Department of Agriculture.

2.2.2. Department of Commerce.

2.2.3. Department of Interior.

2.2.4. Department of Justice.

2.2.5. Department of Labor.

2.2.6. Department of State.

2.2.7. Department of Transportation.

2.2.8. Department of Treasury.

2.2.9. Environmental Protection Agency.

2.2.10. Federal Emergency Management Agency.

2.2.11. Federal Reserve System.

2.2.12. General Accounting Office.

2.2.13. General Services Administration.

2.2.14. National Aeronautics and Space Administration.

2.2.15. National Science Foundation.

2.2.16. Small Business Administration.

2.2.17. United States Arms Control and Disarmament Agency.

2.2.18. United States Information Agency.

2.2.19. United States International Trade Commission.

2.2.20. United States Trade Representative.

2.3. Applies to cases that the Defense Industrial Security Clearance Office (DISCO) forwards to the Defense Office of Hearings and Appeals (DOHA), Defense Legal Services Agency for action under this Directive to determine whether it is clearly

consistent with the national interest to grant or continue a security clearance for the applicant.

2.4. Provides a program that may be extended to other security cases at the direction of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)).

2.5. Does not apply to cases in which:

2.5.1. A security clearance is withdrawn because the applicant no longer has a need for access to classified information;

2.5.2. An interim security clearance is withdrawn by the DISCO during an investigation; or

2.5.3. A security clearance is withdrawn for administrative reasons that are without prejudice as to a later determination of whether the grant or continuance of the applicant's security clearance would be clearly consistent with the national interest.

2.6. Does not apply to cases for access to sensitive compartmented information or a special access program.

3. DEFINITIONS

3.1. Applicant. Any U.S. citizen who holds or requires a security clearance or any immigrant alien who holds or requires a limited access authorization for access to classified information needed in connection with his or her employment in the private sector; any U.S. citizen who is a direct-hire employee or selectee for a position with the North Atlantic Treaty Organization (NATO) and who holds or requires NATO certificates of security clearance or security assurances for access to U.S. or foreign classified information; or any U.S. citizen nominated by the Red Cross or United Service Organizations for assignment with the Military Services overseas. The term "applicant" does not apply to those

U.S. citizens who are seconded to NATO by U.S. Departments and Agencies or to U.S. citizens recruited through such Agencies in response to a request from NATO.

3.2. Clearance Decision. A decision made in accordance with this Directive concerning whether it is clearly consistent with the national interest to grant an applicant a security clearance for access to Confidential, Secret, or Top Secret information. A favorable clearance decision establishes eligibility of the applicant to be granted a security clearance for access at the level governed by the documented need for such access, and the type of investigation specified for that level in DoD 5200.2-R (reference (b)). An unfavorable clearance decision denies any application for a security clearance and revokes any existing security clearance, thereby preventing access to classified information at any level and the retention of any existing security clearance.

4. POLICY

It is DoD policy that:

4.1. All proceedings provided for by this Directive shall be conducted in a fair and impartial manner.

4.2. A clearance decision reflects the basis for an ultimate finding as to whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant.

4.3. Except as otherwise provided for by E.O. 10865 (enclosure 1) or this Directive, a final unfavorable clearance decision shall not be made without first providing the applicant with:

4.3.1. Notice of specific reasons for the proposed action.

4.3.2. An opportunity to respond to the reasons.

4.3.3. Notice of the right to a hearing and the opportunity to cross-examine persons providing information adverse to the applicant.

4.3.4. Opportunity to present evidence on his or her own behalf, or to be represented by counsel or personal representative.

4.3.5. Written notice of final clearance decisions.

4.3.6. Notice of appeal procedures.

4.4. Actions pursuant to this Directive shall cease upon termination of the applicant's need for access to classified information except in those cases in which:

4.4.1. A hearing has commenced;

4.4.2. A clearance decision has been issued; or

4.4.3. The applicant's security clearance was suspended and the applicant provided a written request that the case continue.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Establish investigative policy and adjudicative standards and oversee their application.

5.1.2. Coordinate with the General Counsel of the Department of Defense (GC, DoD) on policy affecting clearance decisions.

5.1.3. Issue clarifying guidance and instructions as needed.

5.2. The General Counsel of the Department of Defense shall:

5.2.1. Establish guidance and provide oversight as to legal sufficiency of procedures and standards established by this Directive.

5.2.2. Establish the organization and composition of the DOHA.

5.2.3. Designate a civilian attorney to be the Director, DOHA.

5.2.4. Issue clarifying guidance and instructions as needed.

5.2.5. Administer the program established by this Directive.

5.2.6. Issue invitational travel orders in appropriate cases to persons to appear and testify who have provided oral or written statements adverse to the applicant relating to a controverted issue.

5.2.7. Designate attorneys to be Department Counsels assigned to the DOHA to represent the Government's interest in cases and related matters within the applicability and scope of this Directive.

5.2.8. Designate attorneys to be Administrative Judges assigned to the DOHA.

5.2.9. Designate attorneys to be Administrative Judge members of the DOHA Appeal Board.

5.2.10. Provide for supervision of attorneys and other personnel assigned or attached to the DOHA.

5.2.11. Develop and implement policy established or coordinated with the GC, DoD, in accordance with this Directive.

5.2.12. Establish and maintain qualitative and quantitative standards for all work by DOHA employees arising within the applicability and scope of this Directive.

5.2.13. Ensure that the Administrative Judges and Appeal Board members have the requisite independence to render fair and impartial decisions consistent with DoD policy.

5.2.14. Provide training, clarify policy, or initiate personnel actions, as appropriate, to ensure that all DOHA decisions are made in accordance with policy, procedures, and standards established by this Directive.

5.2.15. Provide for maintenance and control of all DOHA records.

5.2.16. Take actions as provided for in subsection 6.2., below, and the additional procedural guidance in enclosure 3.

5.2.17. Establish and maintain procedures for timely assignment and completion of cases.

5.2.18. Issue guidance and instructions, as needed, to fulfill the foregoing responsibilities.

5.2.19. Designate the Director, DOHA to implement paragraphs 5.2.5. through 5.2.18., above, under general guidance of the GC, DoD.

5.3. The Heads of the DoD Components shall provide (from resources available to the designated DoD Component) financing, personnel, personnel spaces, office facilities, and related administrative support required by the DOHA.

5.4. The ASD(C3I) shall ensure that cases within the scope and applicability of this Directive are referred promptly to the DOHA, as required, and that clearance decisions by the DOHA are acted upon without delay.

6. PROCEDURES

6.1. Applicants shall be investigated in accordance with the standards in DoD 5200.2-R (reference (b)).

6.2. An applicant is required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed by the DOHA to reach a clearance decision and to otherwise comply with the procedures authorized by this Directive. The applicant may elect on constitutional or other grounds not to comply; but refusal or failure to furnish or authorize the providing of relevant and material information or otherwise cooperate at, any stage in the investigation or adjudicative process may prevent the DOHA from making a clearance decision. If an applicant fails or refuses to:

6.2.1. Provide relevant and material information or to authorize others to provide such information; or

6.2.2. Proceed in a timely or orderly fashion in accordance with this Directive; or

6.2.3. Follow directions of an Administrative Judge or the Appeal Board; then the Director, DOHA, or designee, may revoke any security clearance held by the applicant and discontinue case processing. Requests for resumption of case processing and reinstatement of a security clearance may be approved by the Director, DOHA, only upon a showing of good cause. If the request is denied, in whole or in part, the decision is final and bars reapplication for a security clearance for 1 year from the date of the revocation.

6.3. Each clearance decision must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria and adjudication policy in enclosure 2, including as appropriate:

6.3.1. Nature and seriousness of the conduct and surrounding circumstances.

6.3.2. Frequency and recency of the conduct.

6.3.3. Age of the applicant.

6.3.4. Motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences involved.

6.3.5. Absence or presence of rehabilitation.

6.3.6. Probability that the circumstances or conduct will continue or recur in the future;

6.4. Whenever there is a reasonable basis for concluding that an applicant's continued access to classified information poses an imminent threat to the national interest, any security clearance held by the applicant may be suspended by the ASD(C3I), with the concurrence of the GC, DoD, pending a final clearance decision. This suspension may be rescinded by the same authorities upon presentation of additional information that conclusively demonstrates

that an imminent threat to the national interest no longer exists. Procedures in enclosure 3 shall be expedited whenever an applicant's security clearance has been suspended pursuant to this subsection.

6.5. Nothing contained in this Directive shall limit or affect the responsibility and powers of the Secretary of Defense or the head of another Department or Agency to deny or revoke a security clearance when the security of the nation so requires. Such authority may not be delegated and may be exercised only when the Secretary of Defense or the head of another Department or Agency determines that the hearing procedures and other provisions of this Directive cannot be invoked consistent with the national security. Such a determination shall be conclusive.

6.6. Additional procedural guidance is in enclosure 3.

7. EFFECTIVE DATE

This Directive is effective March 16, 1992, except those cases in which a statement of reasons has been issued shall be concluded in accordance with DoD Directive 5220.6 (reference (a)).

Enclosures - 3

E1. Executive Order 10865, "Safeguarding Classified Information Within Industry," as amended by Executive Order No. 10909 of January 17, 1961, Executive Order No. 11382 of November 28, 1967, and Executive Order No. 12829 of January 6, 1993"

E2. Paragraph 2-200 and Appendix I, DoD 5200.2-R

E3. Additional Procedural Guidance

E1. ENCLOSURE 1

EXECUTIVE ORDER 10865*

SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY

Source: The provisions of Executive Order 10865 of Feb. 20, 1960, appear at 25 FR 1583, 3 CFR 1959-1963 Comp., p. 398, unless otherwise noted.

WHEREAS it is mandatory that the United States protect itself against hostile or destructive activities by preventing unauthorized disclosure of classified information relating to the national defense; and

WHEREAS it is a fundamental principle of our Government to protect the interests of individuals against unreasonable or unwarranted encroachment; and

WHEREAS I find that the provisions and procedures prescribed by this order are necessary to assure the preservation of the integrity of classified defense information and to protect the national interest; and

WHEREAS I find that those provisions and procedures recognize the interests of individuals affected thereby and provide maximum possible safeguards to protect such interest:

NOW, THEREFORE, under and by virtue of the authority vested in me by the Constitution and statutes of the United States, and as President of the United States and as Commander in Chief of the Armed Forces of the United States, it is hereby ordered as follows:

*Executive Order 10865, signed by President Eisenhower on Feb. 20, 1960, is hereby reprinted as amended by Executive Order No. 10909 of January 17, 1961, Executive Order No. 11382 of November 28, 1967, and Executive Order No. 12829 of January 6, 1993. This is an editorial format prepared by the Directorate for Industrial Security Clearance Review as one convenient source for subsequent changes to Executive Order 10865 and is not intended to be used as a definitive legal authority. This version incorporates amendments through January 6, 1993, by Presidents Dwight D. Eisenhower, Lyndon B. Johnson and George Bush.

SECTION 1. When used in this order, the term "head of a Department" means the Secretary of State, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, the Nuclear Regulatory Commission, the Administrator of the National Aeronautics and Space Administration, and, in section 4, the Attorney General. The term "head of a Department" also means the head of any Department or Agency, including but not limited to those referenced above with whom the Department of Defense makes an agreement to extend regulations prescribed by the Secretary of Defense concerning authorizations for access to classified information pursuant to Executive Order No. 12829.

[Sec. 1 amended by EO 10909 of Jan 17, 1961, 26 FR 508, 3 CFR, 1959-1963 Comp., p. 437; EO 11382 of Nov. 28, 1967, 32 FR 16247, 3 CFR, 1966-1970 Comp., p. 691; EO 12829 of Jan. 6, 1993, 58 FR 3479]

SECTION 2. An authorization for access to classified information pursuant to Executive Order No. 12829 may be granted by the head of a Department or his designee, including, but not limited to, those officials named in section 8 of this order, to an individual, hereinafter termed an "applicant", for a specific classification category only upon a finding that it is clearly consistent with the national interest to do so.

[Sec. 2 amended by EO 12829 of Jan 6, 1993, 58 F4 3479]

SECTION 3. Except as provided in section 9 of this order, an authorization for access to a specific classification category may not be finally denied or revoked pursuant to Executive Order 12829 by the head of a Department or his designee, including, but not limited to, those officials named in section 8 of this order, unless the applicant has been given the following:

(1) A written statement of reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.

(2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.

(3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the Department concerned, an opportunity to appear personally before the head of the Department concerned or his designee, including, but not limited to, those officials named in section 8 of this order,

for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.

(4) A reasonable time to prepare for that appearance.

(5) An opportunity to be represented by counsel.

(6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 on matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.

(7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the Department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.

[Sec. 3 amended by EO 12829 of Jan 6, 1993, 58 FR 3479]

SECTION 4. (a) An applicant shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue except that any such statement may be received and considered without affording such opportunity in the circumstances described in either of the following paragraphs:

(1) The head of the Department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest.

(2) The head of the Department concerned or his special designee for that particular purpose has preliminarily determined, after considering information furnished by the investigative agency involved as to the reliability of the person and the accuracy of the statement concerned, that the statement concerned appears to be reliable and material, and the head of the Department or such special designee has determined that failure to receive and consider such statement would, in view of the level of access sought, be substantially harmful to the national security and that the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information to

be considered shall be made available to the applicant, or (B) due to some other cause determined by the head of the Department to be good and sufficient.

(b) Whenever procedures under paragraph (1) or (2) of subsection (a) of this section are used (1) the applicant shall be given a summary of the information which shall be as comprehensive and detailed as the national security permits, (2) appropriate consideration shall be accorded to the fact that the applicant did not have an opportunity to cross-examine such person or persons, and (3) a final determination adverse to the applicant shall be made only by the head of the Department based upon his personal review of the case.

SECTION 5. (a) Records compiled in the regular course of business, or other physical evidence other than investigative reports, may be received and considered subject to rebuttal without authenticating witnesses, provided that such information has been furnished to the Department concerned by an investigative agency pursuant to its responsibilities

in connection with assisting the head of the Department concerned to safeguard classified information within industry pursuant to this order.

(b) Records compiled in the regular course of business, or other physical evidence other than investigative reports, relating to a controverted issue which, because they are classified, may not be inspected by the applicant, may be received and considered provided that: (1) the head of the Department concerned or his special designee for that purpose has made a preliminary determination that such physical evidence appears to be material, (2) the head of the Department concerned or such designee has made a determination that failure to receive and consider such physical evidence would, in view of the level of access sought, be substantially harmful to the national security, and (3) to the extent that the national security permits, a summary or description of such physical evidence is made available to the applicant.

In every such case, information as to the authenticity and accuracy of such physical evidence furnished by the investigative agency involved shall be considered.

In such instances a final determination adverse to the applicant shall be made only by the head of the Department based upon his personal review of the case.

SECTION 6. The head of a Department of the United States or his representative, may issue, in appropriate cases, invitations and requests to appear and testify in order that the applicant may have the opportunity to cross-examine as provided by this order. Whenever a witness is so invited or requested to appear and testify at a proceeding and the witness is an officer or employee of the Executive Branch of the Government or a member of the Armed Forces of the United States, and the proceeding involves the activity in connection with which the witness is employed, travel expenses and per diem are authorized as provided by the Standard Government Travel Regulations or the Joint Travel Regulations, as appropriate. In all other cases (including non-Government employees as well as officers or employees of the Executive Branch of the Government or members of the Armed Forces of the United states not covered by the foregoing sentence), transportation in kind and reimbursement for actual expenses are authorized in an amount not to exceed the amount payable under Standardized Government Travel Regulations. An Officer or employee of the Executive Branch of the Government or a member of the Armed Forces of the United States who is invited or requested to appear pursuant to this paragraph shall be deemed to be in the performance of his official duties. So far as the national security permits, the head of the investigative agency involved shall cooperate with the Secretary, the Administrator, or the head of the other Department or Agency, as the case may be, in identifying persons who have made statements adverse to the applicant and in assisting him in making them available for cross-examination.

If a person so invited is an officer or employee of the Executive Branch of the Government or a member of the Armed Forces of the United States, the head of the Department or Agency concerned shall cooperate in making that person available for cross-examination.

[Sec. 6 amended by EO 10909 of Jan. 17, 1961, 26 FR 508, 3 CFR, 1959-1963 Comp., p. 437; EO 11382 of Nov. 28, 1967, 32 FR 16247, 3 CFR, 1966-1970 Comp., p. 691; EO 12829 of Jan. 6, 1993, 58 FR 3479]

SECTION 7. Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.

SECTION 8. Except as otherwise specified in the preceding provisions of this order, any authority vested in the head of a Department by this order may be delegated to the deputy of that Department, or the principal assistant to the head of that Department, as the case may be.

[Sec. 8 amended by EO 10909 of Jan 17, 1961, 26 FR 508, 3 CFR, 1959-1963 Comp., p. 437; EO 11382 of Nov. 28, 1967, 32 FR 16247, 3 CFR, 1966-1970 Comp., p. 691; EO 12829 of Jan. 6, 1993, 58 FR 3479]

SECTION 9. Nothing contained in this order shall be deemed to limit or affect the responsibility and powers of the head of a Department to deny or revoke access to a specific classification category if the security of the nation so requires. Such authority may not be delegated and may be exercised only when the head of a Department determines that the procedures prescribed in sections 3, 4, and 5 cannot be invoked consistently with the national security and such determination shall be conclusive.

E2. ENCLOSURE 2

ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY

FOR ACCESS TO CLASSIFIED INFORMATION

E2.1. INTRODUCTION

The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information and/or assignment to sensitive national security positions. They apply to persons being considered for initial or continued eligibility for assignment to sensitive positions and/or access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs) and are to be used by Government Departments and Agencies in all final clearance determinations.

E2.2. ADJUDICATIVE PROCESS

E2.2.1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

E2.2.1.1. The nature, extent, and seriousness of the conduct;

E2.2.1.2. The circumstances surrounding the conduct, to include knowledgeable participation;

E2.2.1.3. The frequency and recency of the conduct;

E2.2.1.4. The individual's age and maturity at the time of the conduct;

E2.2.1.5. The voluntariness of participation;

E2.2.1.6. The presence or absence of rehabilitation and other pertinent behavioral changes;

E2.2.1.7. The motivation for the conduct;

E2.2.1.8. The potential for pressure, coercion, exploitation, or duress; and

E2.2.1.9. The likelihood of continuation or recurrence;

E2.2.2. Each case must be judged on its own merits, and final determination remains the responsibility of the specific Department or Agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

E2.2.3. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

E2.2.3.1. Guideline A: Allegiance to the United States

E2.2.3.2. Guideline B: Foreign influence

E2.2.3.3. Guideline C: Foreign preference

E2.2.3.4. Guideline D: Sexual behavior

E2.2.3.5. Guideline E: Personal conduct

E2.2.3.6. Guideline F: Financial considerations

E2.2.3.7. Guideline G: Alcohol consumption

E2.2.3.8. Guideline H: Drug involvement

E2.2.3.9. Guideline I: Emotional, mental, and personality disorders

E2.2.3.10. Guideline J: Criminal conduct

E2.2.3.11. Guideline K: Security violations

E2.2.3.12. Guideline L: Outside activities

E2.2.3.13. Guideline M: Misuse of Information Technology Systems

E2.2.4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

E2.2.5. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

E2.2.5.1. Voluntarily reported the information

E2.2.5.2. Was truthful and complete in responding to questions;

E2.2.5.3. Sought assistance and followed professional guidance, where appropriate;

E2.2.5.4. Resolved or appears likely to favorably resolve the security concern;

E2.2.5.5. Has demonstrated positive changes in behavior and employment;

E2.2.5.6. Should have his or her access temporarily suspended pending final adjudication of the information.

E2.2.6. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

Attachments - 13

E2.A1. GUIDELINE A, Allegiance to the United States

E2.A2. GUIDELINE B, Foreign Influence

E2.A3. GUIDELINE C, Foreign Preference

E2.A4. GUIDELINE D, Sexual Behavior

E2.A5. GUIDELINE E, Personal Conduct

E2.A6. GUIDELINE F, Financial Considerations

E2.A7. GUIDELINE G, Alcohol Consumption

E2.A8. GUIDELINE H, Drug Involvement

E2.A9. GUIDELINE I, Emotional, Mental, and Personality Disorders

E2.A10. GUIDELINE J, Criminal Conduct

E2.A11. GUIDELINE K, Security Violations

E2.A12. GUIDELINE L, Outside Activities

E2.A13. GUIDELINE M, Misuse of Information Technology Systems

E2.A1. ATTACHMENT 1 TO ENCLOSURE 2

GUIDELINE A

Allegiance to the United States

E2.A1.1.1. The Concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individuals allegiance to the United States.

E2.A1.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A1.1.2.1. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of Government by unconstitutional means;

E2.A1.1.2.2. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

E2.A1.1.2.3. Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any State or subdivision, by force or violence or by other unconstitutional means;

E2.A1.1.2.4. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State.

E2.A1.1.3. Conditions that could mitigate security concerns include:

E2.A1.1.3.1. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

E2.A1.1.3.2. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

E2.A1.1.3.3. Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

E2.A1.1.3.4. The person has had no recent involvement or association with such activities.

E2.A2. ATTACHMENT 2 TO ENCLOSURE 2

GUIDELINE B

Foreign Influence

E2.A2.1.1. The Concern: A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

E2.A2.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A2.1.2.1. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

E2.A2.1.2.1. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

E2.A2.1.2.3. Relatives, cohabitants, or associates who are connected with any foreign government;

E2.A2.1.2.4. Failing to report, where required, associations with foreign nationals;

E2.A2.1.2.5. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

E2.A2.1.2.6. Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

E2.A2.1.2.7. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

E2.A2.1.2.8. A substantial financial interest in a country, or in any foreign-owned or -operated business that could make the individual vulnerable to foreign influence.

E2.A2.1.3. Conditions that could mitigate security concerns include:

E2.A2.1.3.1. A determination that the immediate family member(s), (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

E2.A2.1.3.2. Contacts with foreign citizens are the result of official United States Government business;

E2.A2.1.3.3. Contact and correspondence with foreign citizens are casual and infrequent;

E2.A2.1.3.4. The individual has promptly reported to proper authorities all contacts, requests, or threats from persons or organizations from a foreign country, as required;

E2.A2.1.3.5. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

E2.A3. ATTACHMENT 3 TO ENCLOSURE 2

GUIDELINE C

Foreign Preference

E2.A3.1.1. The Concern: When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

E2.A3.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A3.1.2.1. The exercise of dual citizenship;

E2.A3.1.2.2. Possession and/or use of a foreign passport;

E2.A3.1.2.3. Military service or a willingness to bear arms for a foreign country;

E2.A3.1.2.4. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

E2.A3.1.2.5. Residence in a foreign country to meet citizenship requirements;

E2.A3.1.2.6. Using foreign citizenship to protect financial or business interests in another country;

E2.A3.1.2.7. Seeking or holding political office in the foreign country;

E2.A3.1.2.8. Voting in foreign elections; and

E2.A3.1.2.9. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

E2.A3.1.3. Conditions that could mitigate security concerns include:

E2.A3.1.3.1. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

E2.A3.1.3.2. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

E2.A3.1.3.3. Activity is sanctioned by the United States;

E2.A3.1.3.4. Individual has expressed a willingness to renounce dual citizenship.

E2.A4. ATTACHMENT 4 TO ENCLOSURE 2

GUIDELINE D

Sexual Behavior

E2.A4.1.1. The Concern: Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress or reflects lack of judgment or discretion.1 Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

E2.A4.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A4.1.2.1. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

E2.A4.1.2.2. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

E2.A4.1.2.3. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

E2.A4.1.2.4. Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

E2.A4.1.3. Conditions that could mitigate security concerns include:

E2.A4.1.3.1. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

E2.A4.1.3.2. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

E2.A4.1.3.3. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

1 The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders (Guideline I) in determining how to resolve the security concerns raised by sexual behavior.

E2.A4.1.3.4. The behavior no longer serves as a basis

for coercion, exploitation, or duress.

E2.A5. ATTACHMENT 5 TO ENCLOSURE 2

GUIDELINE E

PERSONAL CONDUCT

E2.A5.1.1. The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

E2.A5.1.1.1. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

E2.A5.1.1.2. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

E2.A5.1.2. Conditions that could raise a security concern and may be disqualifying also include:

E2.A5.1.2.1. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

E2.A5.1.2.2. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

E2.A5.1.2.3. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

E2.A5.1.2.4. Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

E2.A5.1.2.5. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;

E2.A5.1.2.6. Association with persons involved in criminal activity.

E2.A5.1.3. Conditions that could mitigate security concerns include:

E2.A5.1.3.1. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

E2.A5.1.3.2. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

E2.A5.1.3.3. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

E2.A5.1.3.4. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

E2.A5.1.3.5. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

E2.A5.1.3.6. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

E2.A5.1.3.7. Association with persons involved in criminal activities has ceased.

E2.A6. ATTACHMENT 6 TO ENCLOSURE 2

GUIDELINE F

Financial Considerations

E2.A6.1.1. The Concern: An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

E2.A6.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A6.1.2.1. A history of not meeting financial obligations;

E2.A6.1.2.2. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

E2.A6.1.2.3. Inability or unwillingness to satisfy debts;

E2.A6.1.2.4. Unexplained affluence;

E2.A6.1.2.5. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

E2.A6.1.3. Conditions that could mitigate security concerns include:

E2.A6.1.3.1. The behavior was not recent;

E2.A6.1.3.2. It was an isolated incident;

E2.A6.1.3.3. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);

E2.A6.1.3.4. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

E2.A6.1.3.5. The affluence resulted from a legal source; and

E2.A6.1.3.6. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

E2.A7. ATTACHMENT 7 TO ENCLOSURE 2

GUIDELINE G

Alcohol Consumption

E2.A7.1.1. The Concern: Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

E2.A7.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A7.1.2.1. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

E2.A7.1.2.2. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

E2.A7.1.2.3. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

E2.A7.1.2.4. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

E2.A7.1.2.5. Habitual or binge consumption of alcohol to the point of impaired judgment;

E2.A7.1.2.6. Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program

E2.A7.1.3. Conditions that could mitigate security concerns include:

E2.A7.1.3.1. The alcohol related incidents do not indicate a pattern;

E2.A7.1.3.2. The problem occurred a number of years ago and there is no indication of a recent problem;

E2.A7.1.3.3. Positive changes in behavior supportive of sobriety;

E2.A7.1.3.4. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

E2.A8. ATTACHMENT 8 TO ENCLOSURE 2

GUIDELINE H

Drug Involvement

E2.A8.1.1. The Concern:

E2.A8.1.1.1. Improper or illegal involvement with drugs, raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information

E2.A8.1.1.2. Drugs are defined as mood and behavior-altering substances, and include:

E2.A8.1.1.2.1. Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens); and

E2.A8.1.1.2.2. Inhalants and other similar substances,

E2.A8.1.1.3. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

E2.A8.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A8.1.2.1. Any drug abuse (see above definition);

E2.A8.1.2.2. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

E2.A8.1.2.3. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

E2.A8.1.2.4. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

E2.A8.1.2.5. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

E2.A8.1.3. Conditions that could mitigate security concerns include:

E2.A8.1.3.1. The drug involvement was not recent;

E2.A8.1.3.2. The drug involvement was an isolated or aberrational event;

E2.A8.1.3.3. A demonstrated intent not to abuse any drugs in the future;

E2.A8.1.3.4. Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

E2.A9. ATTACHMENT 9 TO ENCLOSURE 2

GUIDELINE I

Emotional, Mental, and Personality Disorders

E2.A9.1.1. The Concern: Emotional, mental, and personality disorders can cause a significant deficit in an individuals psychological, social and occupational functioning.
These disorders are of security concern because they may indicate a defect in judgment, reliability or stability.
A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the Government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

E2.A9.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A9.1.2.1. An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

E2.A9.1.2.2. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g. failure to take prescribed medication;

E2.A9.1.2.3. A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

E2.A9.1.2.4. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

E2.A9.1.3. Conditions that could mitigate security concerns include:

E2.A9.1.3.1. There is no indication of a current problem;

E2.A9.1.3.2. Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission, and has a low probability of recurrence or exacerbation;

E2.A9.1.3.3. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

E2.A10. ATTACHMENT 10 TO ENCLOSURE 2

GUIDELINE J

Criminal Conduct

E2.A10.1.1. The Concern: A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

E2.A10.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A10.1.2.1. Allegations or admission of criminal conduct, regardless of whether the person was formally charged;

E2.A10.1.2.2. A single serious crime or multiple lesser offenses.

E2.A10.1.3. Conditions that could mitigate security concerns include:

E2.A10.1.3.1. The criminal behavior was not recent;

E2.A10.1.3.2. The crime was an isolated incident;

E2.A10.1.3.3. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

E2.A10.1.3.4. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

E2.A10.1.3.5. Acquittal;

E2.A10.1.3.6. There is clear evidence of successful rehabilitation.

E2.A11. ATTACHMENT 11 TO ENCLOSURE 2

GUIDELINE K

Security Violations

E2.A11.1.1. The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

E2.A11.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A11.1.2.1. Unauthorized disclosure of classified information;

E2.A11.1.2.2. Violations that are deliberate or multiple or due to negligence.

E2.A11.1.3. Conditions that could mitigate security concerns include actions that:

E2.A11.1.3.1. Were inadvertent;

E2.A11.1.3.2. Were isolated or infrequent;

E2.A11.1.3.3. Were due to improper or inadequate training;

E2.A11.1.3.4. Demonstrate a positive attitude towards the discharge of security responsibilities.

E2.A12. ATTACHMENT 12 TO ENCLOSURE 2

GUIDELINE L

Outside Activities

E2.A12.1.1. The Concern: Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

E2.A12.1.2. Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:

E2.A12.1.2.1. A foreign country;

E2.A12.1.2.2. Any foreign national;

E2.A12.1.2.3. A representative of any foreign interest;

E2.A12.1.2.4. Any foreign, domestic, or international

organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

E2.A12.1.3. Conditions that could mitigate security concerns include:

E2.A12.1.3.1. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

E2.A12.1.3.2. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

E2.A13. ATTACHMENT 13 TO ENCLOSURE 2

GUIDELINE M

Misuse of Information Technology Systems

E2.A13.1.1. The Concern: Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

E2.A13.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A13.1.2.1. Illegal or unauthorized entry into any information technology system;

E2.A13.1.2.2. Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;

E2.A13.1.2.3. Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

E2.A13.1.2.4. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

E2.A13.1.3. Conditions that could mitigate security concerns include:

E2.A13.1.3.1. The misuse was not recent or significant;

E2.A13.1.3.2. The conduct was unintentional or inadvertent;

E2.A13.1.3.3. The introduction or removal of media was authorized;

E2.A13.1.3.4. The misuse was an isolated event;

E2.A13.1.3.5. The misuse was followed by a prompt, good faith effort to correct the situation.

E3. ENCLOSURE 3

ADDITIONAL PROCEDURAL GUIDANCE

E3.1.1. When the DISCO cannot affirmatively find that

it is clearly consistent with the national interest to grant or continue a security clearance for an applicant, the case shall be promptly referred to the DOHA.

E3.1.2. Upon referral, the DOHA shall make a prompt determination whether to grant or continue a security clearance, issue a statement of reasons (SOR) as to why it is not clearly consistent with the national interest to do so, or take interim actions, including but not limited to:

E3.1.2.1. Direct further investigation.

E3.1.2.2. Propound written interrogatories to the applicant or other persons with relevant information.

E3.1.2.3. Requiring the applicant to undergo a medical evaluation by a DoD Psychiatric Consultant.

E3.1.2.4. Interviewing the applicant.

E3.1.3. An unfavorable clearance decision shall not be made unless the applicant has been provided with a written SOR that shall be as detailed and comprehensive as the national security permits. A letter of instruction with the SOR shall explain that the applicant or Department Counsel may request a hearing. It shall also explain the adverse consequences for failure to respond to the SOR within the prescribed time frame.

E3.1.4. The applicant must submit a detailed written answer to the SOR under oath or affirmation that shall admit or deny each listed allegation. A general denial or other similar answer is insufficient. To be entitled to a hearing, the applicant must specifically request a hearing in his or her answer. The answer must be received by the DOHA within 20 days from receipt of the SOR. Requests for an extension of time to file an answer may be submitted to the Director, DOHA, or designee, who in turn may grant the extension only upon a showing of good cause.

E3.1.5. If the applicant does not file a timely and responsive answer to the SOR, the Director, DOHA, or designee, may discontinue processing the case, deny issuance of the requested security clearance, and direct the DISCO to revoke any security clearance held by the applicant.

E3.1.6. Should review of the applicant’s answer to the SOR indicate that allegations are unfounded, or evidence is insufficient for further processing, Department Counsel shall take such action as appropriate under the circumstances, including but not limited to withdrawal of the SOR and transmittal to the Director for notification of the DISCO for appropriate action.

E3.1.7. If the applicant has not requested a hearing with his or her answer to the SOR and Department Counsel has not requested a hearing within 20 days of receipt of the applicant’s answer, the case shall be assigned to the Administrative Judge for a clearance decision based on the written record. Department Counsel shall provide the applicant with a copy of all relevant and material information that could be adduced at a hearing. The applicant shall have 30 days from receipt of the information in which to submit a documentary response setting forth objections, rebuttal, extenuation, mitigation, or explanation, as appropriate.

E3.1.8. If a hearing is requested by the applicant or Department Counsel, the case shall be assigned to the Administrative Judge for a clearance decision based on the hearing record. Following issuance of a notice of hearing by the Administrative Judge, or designee,

the applicant shall appear in person with or without counsel or a personal representative at a time and place designated by the notice of hearing. The applicant shall have a reasonable amount of time to prepare his or her case. The applicant shall be notified at least 15 days in advance of the time and place of the hearing, which generally shall be held at a location in the United States within a metropolitan area near the applicant's place of employment or residence. A continuance may be granted by the Administrative Judge only for good cause. Hearings may be held outside of the United States in NATO cases, or in other cases upon a finding of good cause by the Director, DOHA, or designee.

E3.1.9. The Administrative Judge may require a pre-hearing conference.

E3.1.10. The Administrative Judge may rule on questions on procedure, discovery, and evidence and shall conduct all proceedings in a fair, timely, and orderly manner.

E3.1.11. Discovery by the applicant is limited to non-privileged documents and materials subject to control by the DOHA. Discovery by Department Counsel after

issuance of an SOR may be granted by the Administrative Judge only upon a showing of good cause.

E3.1.12. A hearing shall be open except when the applicant requests that it be closed, or when the Administrative Judge determines that there is a need to protect classified information or there is other good cause for keeping the proceeding closed. No inference shall be drawn as to the merits of a case on the basis of a request that the hearing be closed.

E3.1.13. As far in advance as practical, Department Counsel and the applicant shall serve one another with a copy of any pleading, proposed documentary evidence, or other written communication to be submitted to the Administrative Judge.

E3.1.14. Department Counsel is responsible for presenting witnesses and other evidence to establish facts alleged in the SOR that have been controverted.

E3.1.15. The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision.

E3.1.16. Witnesses shall be subject to cross-examination.

E3.1.17. The SOR may be amended at the hearing by the Administrative Judge on his or her own motion, or upon motion by Department Counsel or the applicant, so as to render it in conformity with the evidence admitted or for other good cause. When such amendments are made, the Administrative Judge may grant either party's request for such additional time as the Administrative Judge may deem appropriate for further preparation or other good cause.

E3.1.18. The Administrative Judge hearing the case shall notify the applicant and all witnesses testifying that 18 U.S.C. 1001 (reference (c)) is applicable.

E3.1.19. The Federal Rules of Evidence (28 U.S.C. 101 et seq. (reference (d)) shall serve as a guide. Relevant and material evidence may be received subject to rebuttal, and technical rules of evidence may be relaxed, except as otherwise provided herein, to permit the development of a full and complete record.

E3.1.20. Official records or evidence compiled or created in the regular course of business, other than DoD personnel background reports of investigation (ROI), may be received and considered by the Administrative Judge without authenticating witnesses, provided that such information has been furnished by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary of Defense, or the Department or Agency head concerned, to safeguard classified information within industry under E.O. 10865 (enclosure 1.). An ROI may be received with an authenticating witness provided it is otherwise admissible under the Federal Rules of Evidence (28 U.S.C. 101 et seq. (reference (d)).

E3.1.21. Records that cannot be inspected by the applicant

because they are classified may be received and considered by the Administrative Judge, provided the GC, DoD, has:

E3.1.21.1. Made a preliminary determination that such evidence appears to be relevant and material.

E3.1.21.2. Determined that failure to receive and consider such evidence would be substantially harmful to the national security.

E3.1.22. A written or oral statement adverse to the applicant on a controverted issue may be received and considered by the Administrative Judge without affording an opportunity to cross-examine the person making the statement orally, or in writing when justified by the circumstances, only in either of the following circumstances:

E3.1.22.1. If the head of the Department or Agency supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his or her identity would be substantially harmful to the national interest; or

E3.1.22.2. If the GC, DoD, has determined the statement concerned appears to be relevant, material, and reliable; failure to receive and consider the statement would be substantially harmful to the national security; and the person who furnished the information cannot appear to testify due to the following:

E3.1.22.2.1. Death, severe illness, or similar cause, in which case the identity of the person and the information to be considered shall be made available to the applicant; or

E3.1.22.2.2. Some other cause determined by the Secretary of Defense, or when appropriate by the Department or Agency head, to be good and sufficient.

E3.1.23. Whenever evidence is received under items E3.1.21. or E3.1.22., above, the applicant shall be furnished with as comprehensive and detailed a summary of the information as the national security permits.

The Administrative Judge and Appeal Board may make a clearance decision either favorable or unfavorable to the applicant based on such evidence after giving appropriate consideration to the fact that the applicant did not have an opportunity to confront such evidence, but any final determination adverse to the applicant shall be made only by the Secretary of Defense, or the Department or Agency head, based on a personal review of the case record.

E3.1.24. A verbatim transcript shall be made of the hearing. The applicant shall be furnished one copy of the transcript, less the exhibits, without cost.

E3.1.25. The Administrative Judge shall make a written clearance decision in a timely manner setting forth pertinent findings of fact, policies, and conclusions as to the allegations in the SOR, and whether it is clearly consistent with the national interest to grant or continue a security clearance for the applicant.

The applicant and Department Counsel shall each be provided a copy of the clearance decision. In cases in which evidence is received under items E3.1.21. and E3.1.22., above, the Administrative Judge's written clearance decision may require deletions in the interest of national security.

E3.1.26. If the Administrative Judge decides that it is clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the DISCO shall be so notified by the Director, DOHA, or designee, when the clearance decision becomes final in accordance with item E3.1.36., below.

E3.1.27. If the Administrative Judge decides that it is not clearly consistent with the national interest for the applicant to be granted or to retain a security clearance, the Director, DOHA, or designee, shall expeditiously notify the DISCO, which shall in turn notify the applicant's employer of the denial or revocation of the applicant's security clearance. The letter forwarding the Administrative Judge's clearance decision to the applicant shall advise the applicant that these actions are being taken, and that the applicant may appeal the Administrative Judge's clearance decision.

E3.1.28. The applicant or Department Counsel may appeal the Administrative Judge's clearance decision by filing a written notice of appeal with the Appeal Board within 15 days after the date of the Administrative Judge's clearance decision. A notice of appeal received after 15 days from the date of the clearance decision shall not be accepted by the Appeal Board, or designated Board Member, except for good cause. A notice of cross-appeal may be filed with the Appeal Board within 10 days of receipt of the notice of appeal. An untimely cross appeal shall not be accepted by the Appeal Board, or designated Board Member, except for good cause.

E3.1.29. Upon receipt of a notice of appeal, the Appeal Board shall be provided the case record. No new evidence shall be received or considered by the Appeal Board.

E3.1.30. After filing a timely notice of appeal, a written appeal brief must be received by the Appeal Board within 45 days from the date of the Administrative Judge's clearance decision. The appeal brief must state the specific issue or issues being raised, and cite specific portions of the case record supporting any alleged error. A written reply brief, if any, must be filed within 20 days from receipt of the appeal brief. A copy of any brief filed must be served upon the applicant or Department Counsel, as appropriate.

E3.1.31. Requests for extension of time for submission of briefs may be submitted to the Appeal Board or designated Board Member. A copy of any request for extension of time must be served on the opposing party at the time of submission. The Appeal Board, or designated Board Member, shall be responsible for controlling the Appeal Board's docket, and may enter an order dismissing an appeal in an appropriate case or vacate such an order upon a showing of good cause.

E3.1.32. The Appeal Board shall address the material issues raised by the parties to determine whether harmful error occurred. Its scope of review shall be to determine whether or not:

E3.1.32.1. The Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record.

In making this review, the Appeal Board shall give deference to the credibility determinations of the Administrative Judge;

E3.1.32.2. The Administrative Judge adhered to the procedures required by E.O. 10865 (enclosure 1.) and this Directive; or

E3.1.32.3. The Administrative Judge's rulings or conclusions are arbitrary, capricious, or contrary to law.

E3.1.33. The Appeal Board shall issue a written clearance decision addressing the material issues raised on appeal.

The Appeal Board shall have authority to:

E3.1.33.1. Affirm the decision of the Administrative Judge;

E3.1.33.2. Remand the case to an Administrative Judge to correct identified error. If the case is remanded, the Appeal Board shall specify the action to be taken on remand; or

E3.1.33.3. Reverse the decision of the Administrative Judge if correction of identified error mandates such action.

E3.1.34. A copy of the Appeal Board's written clearance decision shall be provided to the parties. In cases in which evidence was received under items E3.1.21. and E3.1.22., above, the Appeal Board's clearance decision may require deletions in the interest of national security.

E3.1.35. Upon remand, the case file shall be assigned to an Administrative Judge for correction of error(s) in accordance with the Appeal Board's clearance decision.

The assigned Administrative Judge shall make a new clearance decision in the case after correcting the error(s) identified by the Appeal Board. The Administrative Judge's clearance decision after remand shall be provided to the parties. The clearance decision after remand may be appealed pursuant to items E3.1.28. to E3.1.35., above.

E3.1.36. A clearance decision shall be considered final when:

E3.1.36.1. A security clearance is granted or continued pursuant to item E3.1.2., above;

E3.1.36.2. No timely notice of appeal is filed;

E3.1.36.3. No timely appeal brief is filed after a notice of appeal has been filed;

E3.1.36.4. The appeal has been withdrawn;

E3.1.36.5. When the Appeal Board affirms or reverses an Administrative Judge's clearance decision; or

E3.1.36.6. When a decision has been made by the Secretary of Defense, or the Department or Agency head, under to item E3.1.23., above. The Director, DOHA, or designee, shall notify the DISCO of all final clearance decisions.

E3.1.37. An applicant whose security clearance has been finally denied or revoked by the DOHA is barred from reapplication for 1 year from the date of the initial unfavorable clearance decision.

E3.1.38. A reapplication for a security clearance must

be made initially by the applicant's employer to the DISCO and is subject to the same processing requirements as those for a new security clearance application. The applicant shall thereafter be advised he is responsible for providing the Director, DOHA, with a copy of any adverse clearance decision together with evidence that circumstances or conditions previously found against the applicant have been rectified or sufficiently mitigated to warrant reconsideration.

E3.1.39. If the Director, DOHA, determines that reconsideration is warranted, the case shall be subject to this Directive for making a clearance decision.

E3.1.40. If the Director, DOHA, determines that reconsideration is not warranted, the DOHA shall notify the applicant of this decision. Such a decision is final and bars further reapplication for an additional one year period from the date of the decision rejecting the reapplication.

E3.1.41. Nothing in this Directive is intended to give an applicant reapplying for a security clearance any greater rights than those applicable to any other applicant under this Directive.

E3.1.42. An applicant may file a written petition, under oath or affirmation, for reimbursement of loss of earnings resulting from the suspension, revocation, or denial of his or her security clearance. The petition for reimbursement must include as an attachment the favorable clearance decision and documentation supporting the reimbursement claim. The Director, DOHA, or designee, may in his or her discretion require additional information from the petitioner.

E3.1.43. Claims for reimbursement must be filed with the Director, DOHA, or designee, within 1 year after the date the security clearance is granted. Department Counsel generally shall file a response within 60 days after receipt of applicant's petition for reimbursement and provide a copy thereof to the applicant.

E3.1.44. Reimbursement is authorized only if the applicant demonstrates by clear and convincing evidence to the Director, DOHA, that all of the following conditions are met:

E3.1.44.1. The suspension, denial, or revocation was the primary cause of the claimed pecuniary loss; and

E3.1.44.2. The suspension, denial, or revocation was due to gross negligence of the Department of Defense at the time the action was taken, and not in any way by the applicant's failure or refusal to cooperate.

E3.1.45. The amount of reimbursement shall not exceed the difference between the earnings of the applicant at the time of the suspension, revocation, or denial and the applicant's interim earnings, and further shall be subject to reasonable efforts on the part of the applicant to mitigate any loss of earnings. No reimbursement shall be allowed for any period of undue delay resulting from the applicant's acts or failure to act. Reimbursement is not authorized for loss of merit raises and general increases, loss of employment opportunities, counsel's fees, or other costs relating to proceedings under this Directive.

E3.1.46. Claims approved by the Director, DOHA, shall be forwarded to the Department or Agency concerned for payment. Any payment made in response to a claim for reimbursement shall be in full satisfaction of any further claim against the United States or any Federal Department or Agency, or any of its officers or employees.

E3.1.47. Clearance decisions issued by Administrative Judges and the Appeal Board shall be indexed and made available in redacted form to the public.

SORT: **5230**.11
DOCI: **DODD 5230**.11
DATE: 19920616
TITL: **DODD 5230**.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, June 16, 1992, USD(P)

Refs: (a) DoD Directive **5230**.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984 (hereby canceled)
(b) DoD Instruction **5230**.17, "Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations," February 17, 1985 (hereby canceled)
(c) National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (short title: National Disclosure Policy (NDP-1)), October 1, 1988
(d) through (t), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a), replaces reference (b), implements reference (c), and updates policy, responsibilities, and procedures governing proposed disclosures of classified military information to foreign governments and international organizations (hereafter referred to as "foreign governments").

B. APPLICABILITY AND SCOPE

This Directive applies to:

1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2. All disclosures of classified military information defined in enclosure 2. Disclosures of military intelligence information, however, also must be in compliance with DoD Directive C-**5230**.23 (reference (d)).

Provided to designated disclosure authorities on a need-to-know basis from the Office of the Director for International Security Programs, Office of the Deputy Under Secretary of Defense for Security Policy (ODUSD(SP)).

3. Classified information involved in munitions license applications processed under DoD Directive 2040.2 and the ITAR (references (e) and (f)).

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

It is U.S. national and DoD policy under NDP-1 (reference (c)) that:

1. Classified military information is a national security asset that shall be protected and shall be shared with foreign governments only when there is a clearly defined benefit to the United States. Disclosures of such information shall be made only when authorized by officials designated under this Directive and then only when all requirements of this Directive are met.

2. An official who has been specifically delegated disclosure authority under section E., below, may authorize disclosures of classified military information to foreign governments in support of a lawful and authorized U.S. Government purpose if the:

a. Official represents the DoD Component that originated the information.

b. Level of classified information to be disclosed does not exceed the classification level delegated by Annex A of reference (c).

c. Criteria and conditions in enclosure 3 are satisfied.

3. The Secretary of Defense and the Deputy Secretary of Defense are the only DoD officials who have original authority to grant exceptions to the policy contained in this Directive. The Secretary of Defense has delegatedauthority to the National Military Information Disclosure Policy Committee (NDPC) to consider and grant requests for exceptions to policy in compliance with reference (c).

4. Classified military information shall not be disclosed to foreign nationals until the appropriate designated disclosure authority receives a security assurance from the recipient foreign government on the individuals who are to receive the information.

5. In accordance with reference (c), it is U.S. policy to avoid creating false impressions of U.S. readiness to make available classified military information, materiel, or technology. Accordingly, designated disclosure authorities of the originating DoD Component, or, when an exception to policy is required, the Secretary of Defense, the Deputy Secretary of Defense or the NDPC must authorize, in advance, proposals to be made to foreign governments that could lead to the eventual disclosure of classified military materiel, technology, or information. Commitments shall not be expressed or implied, and no disclosures shall be made pending the required disclosure decision.

6. Disclosure planning shall include the following:

a. Planning for possible foreign involvement should start at the beginningof the weapon system acquisition process and other programs, to facilitate decisions on the disclosure of classified and controlled unclassified information in support of cooperative programs, foreign participation in

the DoD procurement activities, and foreign sales. The planning shall include consideration of the requirements set forth in DoD Instruction 5000.2, Part 5, Section F (reference (g)).

b. The DoD Components shall use the Technology Assessment/Control Plan in DoD Directive 5530.3 (reference (h)) as the basis for making the stated disclosure decisions in paragraph D.6.a., above, on weapon system programs.

c. A delegation of disclosure authority lefter (DDL) similar to that in enclosure 4 shall be used to provide disclosure guidance to subordinate commands and Agencies and, when applicable, to the DoD contractors.

7. All disclosures and denials of classified military information shall be reported in the Foreign Disclosure and Technical Information System (FORDTIS), in accordance with DoD Instruction **5230**.18 (reference (i)). For denials, disclosure authorities must take special care to record a concise summary of the analysis that led to the denial.

8. Under conditions of actual or imminent hostilities, any Unified or Specified Commander may disclose classified military information through TOP SECRET to an actively participating allied force when support of combined combat operations requires the disclosure of that information. The appropriate U.S. Commander shall notify the Chairman of the Joint Chiefs of Staff of such disclosures. The Chairman of the Joint Chiefs of Staff, in turn, shall notify the Office of the Under Secretary of Defense for Policy, ATTN: Chairman, NDPC, who shall determine any limitations that should be imposed on continuing disclosure of the information. The U.S. Commander shall be informed of any limitations through the Chairman of the Joint Chiefs of Staff.

9. The classified military information that is approved for foreign disclosure shall be transmitted to the intended foreign recipient through government-to-government channels, in accordance with DoD 5200. 1-R, chapter 8 (reference (j)).

E. RESPONSIBILITIES

1. The Under Secretary of Defense for Policy shall:

a. Ensure effective implementation of the National Disclosure Policy and operation of the NDPC under NDP-1 (reference (c)).

c. System Countermeasures. Withhold specific information on system counte-measures susceptibilities or vulnerabilities and counter-countermeasures capabilities, until the sale, lease, loan, or grant is consummated.

d. Operation. Employment. Maintenance. and Training. Mter consummation ofa sale, lease, loan, or grant, classified military information may be disclosed up to the level necessary for operation, eniployment, maintenance, and training.

e. Data Packages. Edit or rewrite data packages to exclude information that is beyond that which has been authorized for disclosure.

(1) The disclosure of technical data for production purposes shall be limited to data that is necessary to produce a specific item that is approved for release to the country that is to receive the data.

(2) The disclosure of technical data for maintenance purposes shall be limited to data that is necessary to perform the level of maintenance that has been authorized for the country that is to receive the data.

5. Foreign Test and Evaluation

& Foreign test and evaluation of the U.S. classified equipment may be authorized when the tests:

(1) Are on an item approved for foreign disclosure by the appropriate disclosure authority. (2) Can be performed at a U.S. installation or under other strict U.S. control that guarantees appropriate safeguards for classified information and classified or unclassified critical technology. b. Exceptions to subparagraph F.5.a.(2), above, such as the transfer of a single classified military item for test and evaluation under foreign security control, may be authorized only when all of the following conditions are fulfilled: (1) There is no transfer of, and the test will not reveal, technology that the United States would not license for manufacture in the foreign country. (2) There is no release of equipment that would not be approved for foreign sale or export to the foreign country, if requested. (3) The release will result in a clearly defined advantage to the United States; for example: (a) Specifically defined avoidance of significant costs or acceleration of programs in development efforts by the United States and its allies.

(b) Advance the objectives of standardization with and among U.S. allies by promoting cooperation in research and development.

(c) Exchange technical and scientific information of common interest on a mutually beneficial basis.

(4) The Secretary of the Military Department concerned, in coordination with the Office of the Under Secretary of Defense (Acquisition), approves the exception as meeting the described conditions in paragraph F.5.b., above. The Chair of the NDPC shall be informed of each exception; the Chair shall notify the NDPC members.

(5) The test is performed under a test and evaluation agreement negotiated under DoD Directive 5530.3 (reference (h)), or a lease arrangement or sales contract containing requisite security controls.

(6) The releases are reported to the FORDS.

6. Foreign Participation in DoD Component Classified Training Activities

a. Receiving Training on U.S. Equipment. A foreign national may receive training on U.S. equipment that is classified or involves classified information, if the equipment is in the inventory of or is to be acquired by the trainee's government after the following:

(1) The prospective trainee's government has concluded an international agreement or signed a purchase agreement with the United States to acquire the equipment and training; or

(2) The Defense Security Assistance Agency has issued an International Military Education and Training (IMET) order for the training.

b. Conducting Training on U.S. Equipment. A foreign national may conduct training on U.S. equipment that is classified or involves classified information, if the item has been sold or otherwise provided to the foreign national's government and the U.S. Government has specifically approved the provisions of such training to any third party that is involved.

c. Third-Country Equipment. Foreign nationals may receive or conduct training on equipment provided by a third-country that is classified or involves third-country classified information only with the prior written consent of the government that provided the equipment.

7. Requests for Classified Documents

a. Disclosure Review. Requests for classified documents by a foreign representative shall be forwarded to the applicable designated disclosure authority of the originating DoD Component for review and approval or denial. The requests shall be processed using the FORDTIS, when practicable.

b. Report to the FORDS. The designated disclosure authority that renders the decision shall report it to the FORDS under DoD Instruction **5230**.18 (reference

c. Reference Lists and Bibliographic Material. To avoid false impressionsand to avoid proliferation of requests for classified military information that is not releasable to the requestor, the DoD Components shall:

(1) When practical, excise references to nonreleasable documents and information from material that may be otherwise released.

(2) Discourage release of documents that are reference lists or are bibliographic. To react favorably to justified foreign requests for information, identify the requestor's specific requirements and provide only the U.S. information that satisfies that requirement and is determined to be releasable.

8. Foreign Access to Information When Participating in U.S. Procurement Programs. Participation consistent with applicable U.S. laws, regulations,and security requirements in DoD procurement initiatives by contractors from countries with which the Department of Defense has agreements that encourage reciprocal participation in defense procurement may include access to classified information consistent with this Directive as follows:

a. Access to Technical Data. Qualified government and industry representatives from those countries shall be given appropriate access to technical data, consistent with this Directive and the ITAR (reference (f)), necessary to bid on the DoD contracts.

b. Disclosure Decisions. Disclosure decisions involving those countries shall be made before the announcement of the procurement (see subsection D.6., above), and the announcement shall describe any restrictions on foreign participation.

c. Participation as Subcontractor. When it is determined that foreign contractors are not authorized to participate in the classified or other sensitive aspects of a potential contract, consideration should be given to their requests for participation in unclassified or less sensitive aspects of the contract as a subcontractor.

d. Requests for Documentation. Requests by foreign entities for classifieor controlled unclassified documentation must be submitted through government channels.

9. NDPC Operations. The following procedures apply to the activities below:

a. Exceptions to NDP-1

(1) Exceptions to NDP-1 (reference (c)), other than those granted by the Secretary of Defense or the Deputy Secretary of Defense, shall be granted only by the NDPC.

(2) All proposed disclosure actions that require decisions by the Secretary of Defense or the Deputy Secretary of Defense shall contain the views of the originating DoD Component or Agency and shall be coordinated with the Chair of the NDPC.

(3) When the Secretary of Defense or the Deputy Secretary of Defense grants an exception to policy, the DoD Component originating or participating in the determination shall notify the Chair of the NDPC so that the exception may be recorded properly and reported promptly to the NDPC members and the National Security Council and recorded in the FORDS.

(4) All other requests for exception to policy shall:

(a) Be forwarded through channels to the designated disclosure authority who represents the requestor's organization on the NDPC.

(b) At a minimum, include the information in enclosure 5.

b. Reporting to the NDPC of Compromises of U.S. Classified Military Information Furnished to Foreign Governments. The DoD Components having knowledge of compromises of U.S. classified information by foreign governments promptly shall inform the originating DoD Component. The originating DoD Component shall conduct a damage assessment and shall provide copies of the completed case report and damage assessment to the Chair of the NDPC. If the originating DoD Component is not known, the Chair of the NDPC shall conduct the damage assessment and prepare the case report. In either situation, the Chair of the NDPC shall provide the NDPC with an evaluation to serve as a basis for determining whether the nature of the compromise requires a change in reference (c).

c. Operation of the NDPC

(1) NDP-1, NDPC Record of Action 001.7/70 (references (c) and (o)), and this Directive govern the DoD Component participation in the NDPC operations.

(2) The DoD Components shall provide qualified personnel to participate on the NDPC security survey teams, when requested. The parent DoD Component shall bear travel and per diem expenses for participants.

(3) The DoD members of NDPC security survey teams shall participate in pre

-departure briefings, all scheduled team activities, and the preparation of all reports and briefings resulting from the security survey.

d. Cooperation with the NDPC. Under the NDP-1 (reference (c)), the Chair of the NDPC acts for and in the name of the Secretary of Defense in carrying out the decisions of the NDPC. All of the DoD Components shall support the Chair's requests for assistance in disclosure matters.

10. Classification Requirements. DoD 5200. 1-R (reference (j))governs classification and safeguarding of classified information. The DoD Components also shall follow the security classification guide for NDP matters in enclosure 6.

G. INFORMATION REQUIREMENTS

The reports referenced in this Directive are exempt from licensing in accordance with paragraph E.4.b. of DoD 7750.5-M (reference (p)).

H. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Under Secretary of Defense for Policy within 120 days.

Donald J. Atwood Deputy Secretary of Defense

Enclosures - 6 1. References 2. Definitions 3. NDP-1 Disclosure Criteria, Conditions, and Limitations 4. The DDL 5. Requests for Exception to Policy 6. Security Classification Guide for NDP (DATA OMITTED)

REFERENCES. continued

(d) DoD Directive C-**5230**.23, "Intelligence Disclosure Policy. (u)," November 18, 1983
(e) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984
(f) Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulations (ITAR)"
(g) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991
(h) DoD Directive 5530.3, "International Agreements," June 11, 1987
(i) DoD Instruction **5230**.18, "The DoD Foreign Disclosure and Technical Information System (FORDTIS)," November 6, 1984
(j) DoD 5200. 1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
(k) Public Law 83-703, "Atomic Energy Act of 1954," August 30, 1954, as amended (Sections 2121, 2153, and 2164 of title 42, United States Code)
(l) DoD 7110. 1-M, "Department of Defense Budget Guidance Manual," May 1990, authorized by DoD Instruction 7110.1, October 30, 1980
(m) DoD Directive 5200.12, "Conduct of Classified Meetings," May 16, 1988
(n) DoD Directive **5230**.20, "Control of Foreign Representatives," June 25, 1984 (o) National Military Information Disclosure Policy Committee Record of Action 001.7/70, "NDPC Detailed Operating Procedures," September 15, 1981
(p) DoD 7750.5-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 7750.5, August 7, 1986
(q) Executive Order 12356, "National Security Information," April 2, 1982
(r) DoD Directive **5230**.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
(s) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
(t) Title 15, Code of Federal Regulations, Parts 730-799, "Export Administration Regulations (EAR)"

DEFINITIONS

1. Classified Military Equipment. Military equipment that is itself classified; contains classified information that may be derived from or revealed by its operation or testing; or will require the disclosure of classified information for operation, employment, maintenance, or training.

2. Classified Military Information. Information originated by or for the Department of Defense or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL, as described in E.O. 12356 (reference (q)). Classified military information may be in oral, visual, or material form and has been subdivided further into the eight categories described below:

a. Category 1 - Organization. Training. and Employment of Military ForcesInformation of a general nature pertaining to tactics, techniques, tactical doctrine, and intelligence and counterintelligence doctrine and techniques. Excluded is information necessary for the operation, training,and maintenance on specific equipment covered under Categories 2 and 3, below.

b. Category 2 - Military Materiel and Munitions. Information on specific items of equipment already in production, or in service, and the information necessary for the operation, maintenance, and training. Items on the U.S. Munitions List fall within this category. This category does not pertain to equipment that is in research and development.

c. Category 3 - Applied Research and Development Information and Materiel Information related to fundamental theories, design, and experimental investigation into possible military applications; it includes engineering data, operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when the equipment has completed suitability testing and has been adopted for use or production.

d. Category 4 - Production Information. Information related to designs, specifications, manufacturing techniques, and such related information necessary to manufacture materiel and munitions.

e. Category 5 - Combined Military Operations. Planning. and Readiness Information necessary to plan, ensure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. It does not include strategic plans and guidance or North American defense information.

f. Category 6 - U.S. Order of Battle. Information pertaining to U.S. forces in a specific are& In general, disclosures of this information are limited to those countries in which U.S. forces are stationed or are in adjacent geographical areas.

g. Category 7 - North American Defense. Information related to plans, operations, programs, and projects, to include data and equipment, directly related to North American defense.

h. Category 8 - Military Intelligence. Information of a military charactepertaining to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the Director of Central Intelligence (DCI).

3. Controlled Unclassified Information. Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes U.S. information that is determined to be exempt from public disclosure in accordance with DoD Directives **5230**.25 and 5400.7 (references (r) and (s)) or that is subject to export controls in accordance with the ITAR (reference (f)) or the EAR (reference (t)).

4. Delegation of Disclosure Authority Letter (DDL). A letter issued by the appropriate designated disclosure authority explaining classification levels, categories, scope, and limitations of information under a DoD Component's disclosure jurisdiction that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate disclosure authorities.

5. Designated Disclosure Authority. An official, at subordinate component level, designated by the Head of a DoD Component or the Component's Principal Disclosure Authority to control disclosures of classified military information by his or her organization

6. Disclosure. Conveying classified information, in any manner, to an authorized representative of a foreign government.

7. Foreign Disclosure and Technical Information System (FORDTIS). An automated system to assist decision makers and analysts in reviewing, coordinating, and reaching decisions concerning proposals to release classified military information, materiel, and technology to foreign governments.

8. Government-to-Government Channels. The principle that classified information and materiel will be transferred by government officials through official channels or through other channels expressly agreed upon by the governments involved. In either case, the information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.

9. Intelligence. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

10. International Organization. An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

11. Joint Information. Military information over which two or more DoD Components, or two or more Federal Departments or Agencies, exercise control, jurisdiction, or security awareness.

12. Meeting. A conference, seminar, symposium, exhibit, convention, training course, or other gathering during which classified or controlled unclassified information is disclosed.

13. Originating DoD Component. The DoD Agency that exercises original classification jurisdiction for classified information.

14. Security Assurance. The written confirmation, requested by and exchanged between governments, of the security clearance level or eligibility for clearance, of their employees, contractors, and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of U.S. classified military information possesses the requisite security clearance and is approved by his or her government for access to information of the security classification involved on behalf of the foreign government and that the recipient will comply with any security requirements specified by the United States. In the case of industrial facilities, the security assurance should include a statement concerning the level of storage capability.

15. Sensitive Compartmented Information. Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

16. Strategic War Plan. A plan for the overall conduct of a war.

NDP-1 DISCLOSURE CRITERIA, CONDITIONS, AND LIMITATIONS

A. Disclosure Criteria. Disclosures of classified military information in Categories 1 through 8 defined in item 2 of enclosure 2 may be made only when all of the criteria listed in subsections A-I. through 5., below, are satisfied. Disclosures in Category 8 also must be in compliance with DoD Directive C-**5230**.23 (reference (d)).

1. Disclosure is consistent with U.S. foreign policy and national security objectives concerning the proposed recipient foreign government. For example:

a. The recipient government cooperates with the United States in pursuanceof military and political objectives that are compatible with those of the United States.

b. A specific U.S. national purpose, diplomatic or military, will be served.

c. The information will be used in support of mutual defense and security objectives.

2. Disclosure is consistent with U.S. military and security objectives. For example:

a. Disclosures of advanced technology, if compromised, will not constitutean unreasonable risk to the U.S. position in military technology and operational capabilities, regardless of the intended recipient.

b. The proposed disclosure reflects the need for striking a proper balancebetween pursuit of our mutual defense and foreign policy objectives on the one hand and the preservation of the security of our military secrets on the other.

3. The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the United States. (The intent of a foreign government to protect U.S. classified military information is established in part by the negotiation of a General Security of Information Agreement or other similar security arrangement. Aforeign government's capability to protect U.S. classified military information normally is determined by the evaluation of embassy security assessments, Central Intelligence Agency risk assessments, National Military Information Disclosure Policy Committee (NDPC) Security Survey Reports, and/or historical precedence.)

4. Disclosures will result in benefits to the United States at least equivalent to the value of the information disclosed. For example:

a. The United States obtains information from the recipient nation on a quid pro quo basis. information about strategic war plans. Requests for such disclosure shall be submitted through the Chairman of the Joint Chiefs of Staff.

2. Specifically Prohibited Disclosures. The following types of classified information are specifically prohibited from disclosure:

a. Classified information officially obtained from a foreign government, except when the information has been conveyed by the government with express written consent to its further disclosure.

b. Combined information without prior agreement of all parties.

c. Joint information without prior agreement of all Departments or Agencies having control or jurisdiction.

d. Information originated by or for another Department or Agency, unless that Department or Agency consents to the disclosure.

e. Intelligence information described in section I, subparagraph 5.c.(2) and section ll, subparagraph 5.b.(7) of NDP-1 (reference (c)).

THE DDL

The following DDL format should be used by the DoD Components: (While all elements identified should be provided in the general order shown, information should be presented in the clearest and easiest-to-use manner. For example, the usefulness of the DDL for complex systems will be enhanced if items 5 and 6 are broken out by major subsystems and software and disclosures are discussed separately.)

TITLE: DATE:

1. CLASSIFICATION: Identify highest classification of information to be disclosed.

2. DISCLOSURE METHODS: E.g., oral, visual, or documentary.

3. CATEGORIES PERMITTED: Specify National Disclosure Policy categories to be disclosed.

4. SCOPE: Specify who is authorized to release material or information, and to whom disclosure is authorized.

5. AUTHORIZED FOR RELEASE AND/OR DISCLOSURE: Describe materiel and/or information that can be released or disclosed.

6. NOT AUTHORIZED FOR RELEASE AND/OR DISCLOSURE: Describe materiel and/or information that cannot be released or disclosed. (In addition to providing specific descriptions of releasable and restricted materiel and information, items 5 and 6 will also specify any conditions or limitations to be imposed; e.g., time-phasing of release, allowable forms for software, identification of items releasable only as finished, tested assemblies, etc.)

7. PROCEDURES: Specify review and release procedures, special security procedures, or protective measures to be imposed.

8. REDELEGATION: Specify the extent of redelegation of authority (if any) permitted to subordinate activities.

REQUESTS FOR EXCEPTION TO POLICY

Requests for an exception to policy shall contain the following elements of information:

1. A concise statement of the action proposed. Include security classification and categories of U.S. classified military information to be disclosed. (For example: "The OUSD(A) member, National Disclosure Policy Committee (NDPC), requests an exception to the National Disclosure Policy to permit the disclosure of SECRET Category 3 (Applied Research and Development Information and Materiel) information to the Government of _____ in support of the negotiation of a Data Exchange Agreement pertaining to surface-to-air missiles.")

2. A precise statement of why an exception to policy is required. (For example: An exception is required because (a) the level of classified information involved exceeds the classification level delegated in Annex A of NDP-1; or (b) the proposed action is not in consonance with policy currently established in Annex B or C of NDP-1; or (c) certain (identify which) of the disclosure criteria or conditions listed in section ll. of NDP-1 are not fully met; or
(d) any or all of the above in combination.)

3. An assessment of how each of the disclosure criteria and conditions in section ll. of NDP-1 shall be met:

a. "Disclosure is consistent with the foreign policy of the United States toward the Government of _____." (A further detailed discussion shall be included to substantiate this statement. Reference shall be made to Presidential, National Security Council, or other high-level policy decisions to support the justification provided. A simple statement such as "the recipient cooperates with the United States in pursuance of military and political objectives" is not sufficient.)

b. "The military security of the United States permits disclosure." (If equipment or technology is involved, there must be a discussion on the result of a compromise on U.S. operational capability or the U.S. position

in military technology. This discussion shall include an analysis of the state of the art regarding the technology involved, the susceptibility of the item to reverse engineering, the capability of the foreign recipient to reverse engineer the item, the foreign availability of the technology or equipment involved, and other governments to whom similar equipment or technology has been released.)

c. "The foreign recipient will afford the information substantially the same degree of security protection given to it by the United States." (If there has been an NDPC Security Survey for the proposed recipient, the conclusion reached therein shall be discussed. In the absence of an NDPC Security Survey, efforts shall be made to obtain, through intelligence channels, a counterintelligence risk assessment or security analysis of the foreign government's security capabilities. The mere statement that "classified information has been released previously to this government and there is no indication that such information has been compromised" is not sufficient.)

d. "Disclosures will result in benefits to the United States at least equivalent to the value of the information disclosed." (For example: (1) if the United States obtains information from the proposed recipient on a quid-pro-quo basis, describe the information and the value to the United States; (2) explain how the exchange of military information for participation in a cooperative project will be advantageous to the United States from a technical or military capability viewpoint; (3) if the development or maintenance of a high degree of military strength and effectiveness on the part of the recipient government will be advantageous to the United States, explain how.)

e. "The disclosure is limited to information necessary to the purpose for which disclosure is made." (For example, if the purpose of the request is for the sale of equipment only, it shall be indicated clearly that research and development data or production know-how is not to be divulged or that documentation will be sanitized.)

4. Any limitations placed on the proposed disclosure in terms of information to be disclosed, disclosure schedules, or other pertinent caveats that may affect NDPC approval or denial of the request. (If disclosures are to be phased or if certain information is not to be released, the phasing or nonreleasable information shall be specified.)

5. A statement that the requested exception is to be either a continuing exception, subject to annual review, or a one-time exception. (A continuing exception usually is associated with a long-term project, such as a coproduction program or military sale when the United States will be obligated to provide life-cycle support. A one-time exception typically isused for a briefing or demonstration or short-term training.)

6. The names and titles of U.S. officials accredited to the requesting foreign government or international organization with whom the proposed exception has been coordinated, as well as the views of the Theater Commander. (Sufficient time shall be allowed to obtain an opinion from U.S. Embassy personnel in-country and the responsible Theater Commander before submitting the request for approval. Many cases are delayed becausea U.S. Embassy or Theater Commander opinion has not been obtained.) 7. The opinion of other interested Departments or Agencies if joint Service or shared information is involved. (If the information or item of equipment is of shared or joint interest, such as an air-to-air missile used by two Services or containing technology of concern to another Service, the views of the other party will be included.) 8. Any information not mentioned above that would assist the NDPC members, the Secretary of Defense, or the Deputy Secretary of Defense in evaluating the proposal.

9. The name and telephone number of a knowledgeable individual within the requesting organization who can provide additional technical detail or clarification concerning the case at issue.

10. The date a response is desired on the case. Ten full working days for NDPC case deliberations should be allowed. The suspense date (10 full working days) is computed starting from the first full working day after the date of the request.

<<|IMAGE DODD0409.gif|>>

<<|IMAGE DODD0410.gif|>>

<<|IMAGE DODD0411.gif|>>

SORT: 5240.3

DOCI: DODD 5240.3

DATE: 19830125

TITL: DODD 5240.3 Counterintelligence and Operations Security Support Program for the Defense Nuclear Agency, January 25, 1983, ASD(C3I), thru Ch1, August 7, 1992

References: (a) DoD Directive 5240.2, "Department of Defense Counterintelligence," June 6, 1983

(b) DoD 5240.I-R, "Procedures Governing the Activities of DoD **Intelligence** Components That Affect United States Persons," December 1982, authorized by DoD Directive 524O.1, April 25, 1988

(c) "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation," April 5, 1979

(d) through (i), see enclosure 1

A. PURPOSE

This Directive establishes the counterintelligence (CI)and operations security (OPSEC) support program for the Defense Nuclear Agency (DNA).

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, and the DNA.

C. DEFINITION

CI and OPSEC Support Services. Activities designed to protect classified and operationally sensitive unclassified information and material. Included are CI investigations, counterespionage and countersabotage operations, OPSEC analyses, technical surveillance countermeasures (TSCM) services, CI security education, and CI security assistance.

D. POLICY

It is the policy of the Department of Defense to protect to the maximum the security of the DNA and its field activities. To accomplish this mission effectively, provisions shall be made for a dedicated, tailored CI and OPSEC support program to be administered by the Department of the Army.

E. RESPONSIBILITIES

1. The Deputy Assistant Secretary of Defense (Counterintelligence and

Security Countermeasures) (DASD(CI&SCM)) shall oversee the DNA CI and 0PSEC support pogrom (see DoD Directive 5240.2, reference (a)) and shall designate the Director, counterintelligence, Office of the DASD(CI&SCM), who shall:

a. Conduct an active oversight program to ensure maximum fulfillment of DNA CI and OPSEC support requirements.

b. Review and rule on CI and 0PSEC matters involving the DNA that raise substantial policy issues.

c. Monitor actions taken to correct CI and 0PSEC deficiencies at the DNA and recommend alternative or additional CI and 0PSEC measures.

2. The Secretary of the Army shall:

a. Determine, through coordination with the Director, DNA, the nature and scope of DNA CI and OPSEC support requirements and changes affecting susupport after the changes are reviewed by the DASD(CI&SCM), or designee.

b. Establish and maintain a unit to provide dedicated, tailored CI and 0PSEC support services to the DNA and its field activities. The Commander of this Army CI and 0PSEC support unit shall:

(1) Perform tasks initiated by the Director, DNA, or designee, in accordance with established security and investigative policy and procedures. Any tasks requiring the Secretary of the Army's approval shall be forwarded through channels to the Office of the Deputy Chief of Staff for **Intelligence**.

(2) Advise the Director, DNA, and appropriate DNA subordinate commanders on matters affecting the security of the DNA.

(3) Collect threat information within the limitations established in DoD 5240.1-R (reference (b)) to provide the DNA with early warnings of threats.

(4) Report threat data and security hazards promptly to the Director, DNA, or designee, providing evaluation and analysis within the Army's capabilities.

(5) Refer CI matters involving military personnel assigned to the DNA to the military CI agency of the Military Department concerned for appropriate investigation and disposition. Counterespionage and countersabotage operations may use military personnel as principals only with the concurrence of the military CI agency of the Military Department concerned.

(6) Refer CI matters involving civilian employees of the DNA to the Federal Bureau of Investigation (FBI) for investigation and disposition, in accordance with the "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation" (reference (c)).

(7) Provide OPSEC support, advice, and assistance, in accordance with JCS Pub 18 (reference (d)).

(8) Coordinate automated systems security support in accordance with DoD Directive 5200.28 (reference (e)).

(9) Provide TSCM support in accordance with DoD Instruction 5240.5 (reference (f)).

(10) Conduct **intelligence** liaison, OPSEC support liaison, and combined OPSEC support operations directly with the Department of Energy (DoE) and the Nuclear Regulatory Commission (NRC) at those locations and installations and on those projects in which the DNA, DoE, and NRC work together.

(11) Establish and maintain direct channels of communications with the Defense **Intelligence** Agency, Central **Intelligence** Agency, NRC, DoE, and **intelligence** and counterintelligence activities of the Military Departments to obtain and exchange information to support DNA mission requirements.

(12) Maintain direct contact with the FBI to obtain information on nuclear-related incidents and violations of the Atomic Energy Act of 1954 (reference (g)), nuclear terrorism, and other matters concerning the security of the DNA and its field activities.

3. The Director, Defense Nuclear Agency, shall:

a. Develop and implement appropriate security plans in accordance with DoD Directives 5200.1 and 5200.2 (references (h) and (i)).

b. Submit CI and OPSEC tasking requirements directly to-the Commander of the Army Cl and OPSEC support unit.

c. Take corrective actions on security deficiencies and hazards reported by the Army CI and 0PSEC support unit.

d. Provide the Army CI and 0PSEC support unit with necessary administrative personnel actions and logistics support on a nonreimbursable basis.

F. EFFECTIVE DATE

This Directive is effective immediately.

Deputy Secretary of Defense

Enclosure - 1

References

REFERENCES (continued)

(d) JCS Pub 354, "Joint Doctrine for Operations Security (u)," August 22, 1991
(e) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
(f) DoD Instruction 5240.5, DoD Technical Surveillance Countermeasures (TSCM) Survey Program," May 23, 1984

(g) Public Law 83-703, Atomic Energy Act of 1954, as amended

(h) DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982

(i) DoD Directive 5200.2, "DoD Personnel Security Program," May 6, 1992

Department of Defense

DIRECTIVE

NUMBER 8520.1

December 20, 2001

ASD(C3I)

SUBJECT: Protection of Sensitive Compartmented Information (SCI)

References: (a) Section 403-5(a) of title 50, United States Code, "National Security"

(b) Executive Order 12333, "United States Intelligence Activities," December 4, 1981

(c) DoD 5200.2-R, "DoD Personnel Security Program Regulation," January 1987

1. PURPOSE

This Directive implements reference (a) to establish policy and assign responsibilities regarding the protection, use, and dissemination of Sensitive Compartmented Information (SCI) within the Department of Defense.

2. APPLICABILITY AND SCOPE

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

3. DEFINITIONS

3.1. Intelligence Community and Agencies Within the Intelligence Community. Consistent with Section 3 of reference (a) and Section 3.4(f)(1 through 6) of Executive Order 12333 (reference (b)) the Intelligence Community and agencies within the Intelligence Community refer to the following agencies or organizations: the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Imagery and Mapping Agency, the National Reconnaissance Office, the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs, the Bureau of Intelligence and Research of the Department of State, the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Federal Bureau of Investigation, the Department of the Treasury, and the Department of Energy.

3.2. Senior Officials of the Intelligence Community

(SOICs). Consistent with Section 1.7 of Executive Order 12333 (reference (b)), Senior Officials of the Intelligence Community are the heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, as specified in DCI Directives.

3.3. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI).

3.4. Senior Intelligence Officer (SIO). The highest ranking military or civilian charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, or element of an Intelligence Community organization.

4. POLICY

It is DoD policy that:

4.1. SCI shall be safeguarded in accordance with policies and procedures established by the DCI. Nothing in this Directive is intended to diminish the authority and responsibility of the DCI over SCI or individual SOICs.

4.2. All DoD Components with responsibility for protecting SCI will establish and foster partnerships with elements of the DoD SCI community, the DCI, industry, and professional associations to gain insight to establishing common security practices and reciprocity wherever practicable.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.1.1. Serve as the senior DoD official responsible for oversight of implementation of SCI security policies and procedures within the Department of Defense.

5.1.2. Represent the Secretary of Defense in coordination of SCI security policies and procedures established by the DCI.

5.2. The Director, National Security Agency, Director, National Reconnaissance Office, and Director, National Imagery and Mapping Agency shall establish, direct, and administer all aspects of their respective organization's SCI security programs to include all necessary coordination and implementation of DCI security policy.

5.3. The Director, Defense Intelligence Agency shall:

5.3.1. Administer within the Department of Defense, with the exception of NSA and NRO, SCI security policies and procedures issued by the DCI. As a minimum, this includes responsibility for:

5.3.1.1. Ensuring that SCI security policies and procedures issued by the DCI, and all DCI-issued changes or modifications thereto, are disseminated within the Department of Defense in a timely and efficient manner.

5.3.1.2. Inspecting and accrediting DoD and DoD contractor facilities for the handling, processing, storage and discussion of SCI.

5.3.1.3. Inspecting DoD and DoD contractor-accredited SCI facilities on a recurrent basis to determine continued compliance with established SCI security policies and procedures and issuance of reports detailing any deficiencies

noted and corrective action required.

5.3.1.4. Preparing and submitting such reports as may be required by the DCI and/or the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) regarding the status of implementation of SCI security policies and procedures within the Department of Defense.

5.3.1.5. Adjudicating eligibility for access to SCI for all civilian personnel assigned to DIA, the Office of the Secretary of Defense, the Joint Staff, the Defense Agencies and the DoD Field Activities, including contractors and consultants, and military personnel assigned to DIA, in accordance with DoD 5200.2-R (reference (c)).

5.3.1.6. Monitoring SCI personnel security practice to include leading program reviews and conducting inspections of adjudication facilities to ensure standardization of SCI personnel security practices.

5.3.1.7. Monitoring the establishment and maintenance of SCI security awareness and education programs within the DoD Components.

5.3.1.8. Developing and coordinating within the Department of Defense recommendations with respect to current or proposed DCI SCI security policy and procedures.

5.3.1.9. Establishing Memoranda of Agreement for joint DoD use of CIA, NSA, and NRO SCI-accredited contractor facilities by the DoD Components and their subordinate elements.

5.3.1.10. Operating SCI security programs to support other DoD activities and Federal Agencies by special agreement, as required.

5.4. The Head of each DoD Component that does not have a Senior Official of the Intelligence Community (SOIC) shall designate at appropriate levels, Senior Intelligence Officers who shall be responsible for the effective implementation of SCI security policies and security awareness and education programs within the Component.

5.5. DoD Senior Officials of the Intelligence Community and Senior Intelligence Officials Designated Under paragraph 5.4., above, shall:

5.5.1. Protect intelligence and intelligence sources and methods from unauthorized disclosure and administer SCI security programs within their respective organizations, consistent with guidance established by the DCI.

5.5.2. Be responsible for ensuring that adequate funding and other resources are available for effective implementation of SCI security policies and procedures and associated security awareness and education programs within the Component.

6. EFFECTIVE DATE

This Directive is effective immediately.

SORT: 8910.01
DOCI: **DODD** 8910.1
DATE: 19930611
TITL: **DODD** 8910.1 Management and Control of Information Requirements, June 11, 1993, ASD(C3I)

Refs: (a) DoD Directive 7750.5, subject as above, August 7, 1986 (hereby canceled)
(b) DoD Directive 8000.1, "Defense Information Management (lM) Program," October 27, 1992
(c) Public Law 96-511, "The Paperwork Reduction Act of 1980," December 11, 1980, as amended (44 U.S.C. 350 et sea.)
(d) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by this Directive
(e) through (q), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive:

1. Administratively renumbers and reissues reference (a).

2. Establishes policy and assigns responsibilities for the management and control of information requirements and implements those policies in references (b) and (c) on the licensing of reporting requirements internal and external to the Department of Defense and the development of an information collection budget.

3. Continues to authorize publication of DoD 7750.5-M, hereby changed to DoD 8910.1-M (reference (d)), and DoD 7750.5-L, hereby changed to DoD 8910.1-L (reference (e)), in accordance with DoD 5025.1-M (reference (f)).

B. APPLICABILITY AND SCOPE

This Directive:

1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments (including the National Guard and Reserve components), the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2. Applies to existing, revised, and new information requirements (internal DoD, inter-Agency, and public reporting requirements) and the systems and processes necessary to support them. All information and reporting systems and all techniques (electronic and manual) for collecting, recording, maintaining, and disseminating information for all functional areas are included under its provisions unless specifically exempted by reference (c).

3. Encompasses the information requirements developed in support of all management functions, unless excluded in reference (d)1 and includes information collected to satisfy statutory, congressional, and other inter -Agency imposed information requirements; the collection of information from sources external to the Federal Government; and information collected internally within the Department of Defense.

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

1. Ensuring that sufficient information is available to achieve military effectiveness and management efficiency is a basic command and management responsibility. As a fundamental policy, however, the burden associated with the collection and reporting of this information must be controlled and minimized. The management of reports internally prescribed by the DoD Component must include provision for setting annual goals, consistent with critical mission needs, to reduce the number or frequency of reports.

2. The central ingredient in information management is the user's responsibility and accountability for ensuring that information requirements are valid, accurate, and essential to the mission of the users organization.

a. Information requirements should be examined to avoid both duplication and unnecessary generation of data. Because the creation or collection of information requires the allocation of scarce resources, the user must first ascertain that the required data are not already available from other sources.

b. Statistical sampling techniques and information technology should be emphasized as approaches for minimizing reporting workloads.

c. In the development and operational life cycle of an automated information system, care shall be taken to ensure that information needs are clearly identified and that reports to be generated by the automated system represent cost-effective use of resources, as required by DoD Directive 8120.1 (reference (g)).

3. Information collected from the public (individuals, businesses, and other private institutions) and State and local governments shall also be minimized, accounted for, and controlled. Section 1320 of 5 CFR (reference(h)) directs that public information collections be submitted to the Office of Management and Budget (OMB) for approval, and that an annual information collection budget of burden hours be developed and submitted to the OMB.

4. To ensure optimum effectiveness and economy in the development of information requirements, the following guidance shall be applied:

a. Each new or revised information requirement shall be subjected to a cost analysis. An estimate or actual cost of obtaining the information shall be developed by the requester in accordance with DoD 8910.1-M (reference (d)). A full cost-benefit analysis shall be required for all information collections and systems that are considered to be major by a senior information resources management (IRM) official or representative.

b. Each item of data in the information requirement shall be evaluated andscreened against data in existing information collections to determine whether such information can satisfy the requirement. Information requirements shall be designed to meet only essential needs and be in the minimal frequency feasible, with reasonable due dates. The number of copies to be prepared shall be held to a minimum. Repetitive one-time information requirements may not be imposed when the need for a recurring information requirement is indicated.

c. Information requirements shall comply with existing standard data elements and codes published in DoD 5000.12-M (reference (i)). If required data elements and codes do not exist, they shall be standardized, when appropriate, consistent with DoD Directive 8320.1 (reference (j)).

d. Internal DoD information requirements shall be approved and symbolized;i.e., assigned an information requirement control symbol at the organizational Component level generating the requirement.

e. Information requirements that have not been properly approved and symbolized shall not be honored. The office requesting the data shall be notified that an information requirement control symbol must be obtained before the data can be collected.

r f. Information requirements that involve the collection of personal information on individuals require special handling under DoD Directive 5400.11 (reference (k)). Information or data included in the proposed information requirement shall be accessible to the public, only as prescribed by DoD Directive 5400.7 (reference (l)).

g. On an individual case-by-case basis, special one-time, high priority, or time-urgent requirements may be approved and symbolized without being subjected to in-depth review and analysis, provided a statement of urgency is included with the request for approval document. It will be the responsibility of the requester to complete the request for approval document retroactively, including the appropriate justification and cost estimates.

5. To ensure that ongoing information requirements are still valid and adequate, users shall perform assessments of their ongoing information requirements no less frequently than every 3 years. Actions shall be takento accomplish modifications, cancellations, or new initiatives identified during the review. The DoD Components should consider the assignment of expiration dates to reports as a means of distributing the workload of relicensing reports.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence as the DoD senior official responsible for implementing Pub.L. No. 96-511 1980 reference (c)), shall, consistent with the guidance prescribed by the OMR.

a. Develop and issue DoD-wide policies for the management, control, and registration of internal DoD, inter-Agency, and public reporting requirements.

b. Establish goals, as appropriate, consistent with critical mission needs, for reduction in the number and frequency of OSD-prescribed internal reports.

c. Oversee accomplishment of all DoD report reduction goals.

d. Provide policy oversight and monitor the information collection budget.
e. Approve and publish DoD 8910.1-M (reference (d)), in accordance with DoD 5025.1-M (reference (f)).

2. The Assistant Secretary of Defense (Production and Logistics) shall review and administer data requirements acquired by solicitation or contract, and publish and maintain DoD 5010.12-L(reference (m)), in accordance with DoD Instruction 5000.2 (reference (n)).

3. The Assistant Secretary of Defense (Force Management and Personnel) shall, before submission to the Director, Washington Headquarters Services (WHS), approve surveys requiring participation of personnel in any DoD Component, other than the sponsoring Component, as prescribed by DoD Instruction 1100.13 (reference (o)).

4. The Director, Washington Headquarters Services, shall:

a. Develop and coordinate DoD 8910.1-M (reference (d)) to provide procedures governing the processing, review, and approval of information requirements (DoD internal, interagency, and public reports).

b. Establish an OSD information requirements control activity to:

(1) Maintain and distribute an index of approved information requirements (DoD 8910.1-L (reference (e))).

(2) Maintain the data profiles of all DoD public, inter-Agency, and OSD-prescribed internal reports on an automated locator system. This system should be compatible with the Federal Information Locator System established by Pub. L. No. 96-511(1980) (reference (c)).

(3) Serve as the DoD reviewing office and the office of record for interagency information requirements imposed by the Department of Defense or by external agencies, in accordance with the Federal Information Resources Management Regulation (FIRMR) (reference (p)).

(4) Serve as the DoD clearance office and the office of record for DoD public reporting, in accordance with Pub. L. No. 96-511(1980) (reference (c)) and 5 CFR 1320 (reference (h)).

(5) Serve as the office of record and approval authority for OSD-prescribed internal information requirements, in accordance with the FIRMR (reference (p)).

c. Take appropriate action on the results of OSD staff assessments of

their ongoing information requirements.

5. The Secretaries of the Military Departments the Chairman of the Joint Chiefs of Staff and the Directors of the Defense Agencies shall:

a. Ensure that users justify new information requirements before submission for approval to ensure that the data are not already available from other sources.

b. Establish an information requirements control activity under their senior IRM official or representative to:

(1) Serve as the principal point of contact on the various information requirements programs.

(2) Provide for the efficient and effective management and control of information requirements.

(3) Process, assign, and cancel internal information requirement control symbols where applicable. Information requirement control symbols assignedby a higher level shall not be assigned a different information requirement control symbol by a lower level organization.

(4) Submit their respective information collection budgets to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C31)).

(5) Submit their requests for public and interagency information requirements to the Director, WHS.

(6) Maintain an up-to-date index of their approved information requirements.

c. Respond only to those information requirements that have been symbolized; that is, assigned an information requirement control symbol, an inter-Agency report control number, or an OMB approval number, or exempted, consistent with DoD 8910.1-M (reference (d)).

d. Maintain cost information consistent with paragraph D.4.a., above. Wheappropriate, cost information shall also be maintained at other levels of command.

e. Establish goals, as appropriate, consistent with critical mission needs, for reduction in the number or frequency of their internally prescribed reports.

f. Ensure that users assess their ongoing information requirements no lessfrequently than every 3 years, take appropriate action, and communicate the results of their actions to the information requirements control activity.

6. The OSD Principal Staff Assistants shall:

a. Designate an information management control officer for their respective functional areas.

b. Submit their information requirement requests to the Director, WHS.

c. Respond only to those public and inter-Agency information requirements that have valid control numbers.

d. Submit their respective information collection budgets to the ASD(C31).
e. Assess their ongoing information requirements no less frequently than every 3 years and communicate the results of the assessment to the Director, WHS.

F. INFORMATION REQUIREMENTS

The Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the Directors of the Defense Agencies are hereby delegated authority to approve, symbolize, or exempt their own prescribed internal information requirements.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. The Heads of the DoD Components shall keep implementing documents to the absolute minimum. Forward one copy of implementing documents to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence within 120 days.

William J. Perry Deputy Secretary of Defense

Enclosures - 2 1. References 2. Definitions

REFERENCES, continued

(e) DoD 8910.1 -L, "Listing of Approved Recurring Information Requirements," January 1993, authorized by this Directive
(f) DoD 5025.1-M, "DoD Directives System Procedures," December 1990, authorized by DoD Directive 5025.1, December 23, 1988
(g) DoD Directive 8120.1, "Life Cycle Management (LCM) of Automated Information Systems (AISs)," January 14, 1993
(h) Title 5, Code of Federal Regulations, Section 1320
(i) DoD 5000.12-M, "DoD Manual for Standard Data Elements, "July 1989, authorized by DoD Instruction 5000.12, April 27, 1965
(j) DoD Directive 8320.1, "DoD Data Administration," September 26, 1991
(k) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
(l) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
(m) DoD 5010.1 2-L, "Acquisition Management Systems and Data Requirements Control List," October 1992, authorized by DoD Instruction 5000.2, February 23, 1991
(n) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991
(o) DoD Instruction 1100.13, "Surveys of Department of Defense Personnel," November 9, 1978
(p) Federal Information Resources Management Regulation(FIRMR), Part 201-9, April 29, 1991 (Title 41, Code of Federal Regulations, Chapter 201)
(q) Office of Management and Budget (OMB) Circular A-130, "Management of Information Resources, "December 12,1985

DEFINITIONS

1. Information. Any communication or reception of knowledge such as facts,data, or opinions, including numerical, graphic, or narrative forms,

whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. (See OMB Circular A-130, reference (q).)

2. Information Collection Budget. An annual comprehensive budget of burdenhours for all collections of information from the public to be conducted or sponsored by a Federal Agency in the succeeding 12 months.

3. Information Collection Request. A written report form, application formsurvey, schedule, questionnaire, reporting or record keeping requirement, or other similar method calling for the collection of information.

4. Information Requirement. The functional area expression of need for data or information to carry out specified and authorized functions or management purposes that require the establishment or maintenance of forms or formats, or reporting or record keeping systems, whether manual or automated.

5. Information Requirements Assessment. The analysis of ongoing information requirements to ascertain the need for the information, the cycle of reporting, the timeliness of the requirement, the accuracy of the information, and the cost-effectiveness of the requirement.

6. Information Resources Management (IRM). The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by Agencies. The term includes the management of information and related resources, such as Federal information processing resources. (See Pub. L. No. 96-511(1980), reference (c).)

7. OSD Principal Staff Assistants. The Under Secretaries of Defense; the Assistant Secretaries of Defense; the General Counsel of the Department of Defense; the Inspector General of the Department of Defense; the Comptroller of the Department of Defense; the Assistants to the Secretary of Defense; and the OSD Directors, or equivalents, who report directly to the Secretary or the Deputy Secretary of Defense (DoD 5025.1-M, reference (f)). 8. Senior IRM Official or Representative. The term is defined to include the single official for IRM designated under reference (c) and those representatives in the Defense Agencies, designated by their Heads, as responsible for oversight of Agency information matters.

9. Surveys of Persons. Systematic data collections, using personal or telephonic interviews, or self-administered questionnaires, from a sample of 10 or more persons as individuals or representatives of Agencies that elicit attitudes, opinions, behavior, and related demographic, social, and economic data to identical questions that are to be used for statistical compilations for research and/or policy assessment purposes.

SORT: 1025.03
DOCI: DODI 1025.3
DATE: 19930119
TITL: DODI 1025.3 Administrator, National Security Education Program, January 19, 1993, ASD(C3I), thru Ch1, May 13, 1994

References: (a) DoD Directive 5200.3S, "National Security Education Program," January 13, 1993
(b) DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987
(c) Title I of Public Law 98-497, "Public Printing and Documents," October 19, 1984
(d) Charter of the National Security Education Board, June 23, 1992
(e) through (h), see enclosure 1

A. PURPOSE

This Instruction assigns responsibilities, functions, and authorities to the Administrator, National Security Education Program, under reference (a).

B. APPLICABILITY

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

C. RESPONSIBILITIES AND FUNCTIONS

The Administrator, National Security Education Program, shall:

1. Administer, direct, and manage the resources for the program.

2. Establish and direct an international education center, as approved by the Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** (ASD (C3I)), to assist in administering and managing the program. The Center shall be staffed by an appropriate number and type of personnel who, unless otherwise directed by the ASD(C3I), will be subject to Defense **Intelligence** Agency personnel management procedures. Costs that the Agency bears for these personnel shall be reimbursed from the Trust Fund. This staff will be supplemented by contract personnel within the scope of existing law and regulation.

3. Select, approve the hiring of, and evaluate the performance of personnel who staff the international education center.

4. Ensure appropriate internal management controls for the program in accordance with DoD Directive 5010.38 (reference (b)).

5. Carry out a Records Management Review Program under Pub. L. No. 98-497, Title I (reference (c)).

6. Ensure that program activities support the purpose and follow procedures of this Instruction and are carried out in consultation with the National Security Education Board (the Board) or, when the Board is not in session, the Working Group of Board member representatives under the Charter (reference (d)).

7. Ensure that the Board's activities are consistent with DoD Directive 5105.4 (reference (e)).

8. Provide an executive director and establish an executive secretariat to support the Board and its subgroups from resources provided to support the program.

9. Ensure development of the following for Board consideration:

a. Qualifications for applicants for program awards.

b. Critical disciplines in languages, area studies, and other international fields.

c. Criteria for scholarship, fellowship, and grant programs to be offered.

d. Rules for conduct of the program, and regulations for satisfactory student progress and student service agreements.

10. Chair the Board Working Group and call Working Group and advisory subgroup meetings in accordance with the Charter (reference (d))

11. Develop resource requirements for the program and ensure their submission to the DoD Comptroller for inclusion in the Revolving and Management Funds (Trust Funds) subtitle of the DoD budget.

12. Make appropriate arrangements to carry out student service agreements related to the program.

13. Develop rules for handling contributions and voluntary services, as required, to administer the Program.

14. Recommend to the ASD(C3I) any DoD Instructions, Publications, and directive-type memoranda, consistent with DoD 5025.1-M (reference (f)), that are necessary to administer the program.

15. Prepare the annual report to the Congress as specified in Section 806 of Pub. L. No. 102-183, Title VIII (reference (g)).

16. Perform such other duties relating to the program as the ASD(C3I) may assign.

D. AUTHORITIES

The Administrator, National Security Education Program, is specifically delegated the authority to:

1. For program administration, communicate directly with the DoD Components, other Executive Departments and Agencies, representatives of the Legislative and Judicial Branches, public and private sector organizations, educational institutions, and members of the public. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments. Communications to the Commanders of Unified and Specified Combatant Commands shall be transmitted through the Chairman of the Joint Chiefs of Staff.

2. Obtain reports, information, advice, and assistance from the DoD Components, other Executive Departments and Agencies, representatives of the Legislative and Judicial Branches, public and private sector organizations, educational institutions, and members of the public, consistent with DoD Directive 7750.5 (reference (h)), as necessary, to carry out the program.

3. Exercise the administrative authorities in enclosure 2.

E. INFORMATION REQUIREMENTS

The reporting requirements contained in this Instruction are currently under review at the Office of Management and Budget (OMB). An OMB control number will be issued by change to this instruction within 60-90 days.

F. EFFECTIVE DATE

This Instruction is effective immediately.

Enclosures - 2

REFERENCES, continued

(e) DoD Directive 5105.4, "Department of Defense Federal Advisory Committee Management Program," September 5, 1989
(f) DoD 5025.1-M, 1, DoD Directives System Procedures," December 1990, authorized by DoD Directive 5025.1, December 23, 1988
(g) Title VIII of Public Law 102-183, "National Security Education Act of 1991," December 4, 1991, as amended
(h) DoD Directive 7750.5, "Management and Control of Information Requirements," August 7, 1986

DELEGATIONS OF AUTHORITY

Under the authority vested in the Secretary of Defense, and subject to the authority, direction, and control of the Secretary of Defense, and in accordance with DoD policies, Directives, and Instructions, the Administrator, National Security Education Program, or in the absence of the Administrator, the person acting for the Administrator, is hereby delegated authority as required in the administration and operation of the National Security Education Program to:

1. Authorize and approve:

a. Temporary duty travel for military personnel assigned or detailed to the National Security Education Program in accordance with Volume I of the Joint Federal Travel Regulations.

b. Travel for National Security Education Program civilian employees in accordance with Volume II of the Joint Travel Regulations.

c. Invitational travel to non-DoD personnel whose consultative, advisory, or other highly specialized technical services are required in a capacity that is directly related to, or in connection with, National Security Education Program activities, in accordance with Volume II of the Joint Travel Regulations.

d. Overtime work for National Security Education Program civilian employees in accordance with Chapter 55, Subpart V, of 5 U.S.C. and applicable Office of Personnel Management regulations.

2. Approve the expenditure of funds available for travel by military personnel assigned or detailed to the National Security Education Program for expenses incident to attendance at meetings of technical, scientific, professional, or other similar organizations in such instances where the approval of the Secretary of Defense, or designee, is required by 37 U.S.C. 412, and 5 U.S.C. 4110 and 4111.

3. Develop, establish, and maintain an active and continuing Records Management Program under 44 U.S.C. 3102 and DoD Directive 5015.2, "Records Management Program," March 22, 1991.

4. Establish and use imprest funds for making small purchases of material and services, other than personal services, for the National Security Education Program, when it is determined more advantageous and consistent with the best interests of the Government, in accordance with DoD Directive 7360.10, "Disbursing Policies," January 17, 1989.

5. Authorize the publication of advertisements, notices, or proposals in newspapers, magazines, or other public periodicals, as required, for the effective administration and operation of the National Security Education Program, consistent with 44 U.S.C. 3702.

6. Enter into support and service agreements with the Military Departments, other DoD Components, or other Government Agencies, as required, for the performance of National Security Education Program functions and responsibilities.

7. Enter into and administer contracts, directly or through a Military Department, a DoD contract administration service component, or other Federal Agency, as appropriate, for supplies, equipment, and services required to accomplish the mission of the National Security Education Program. To the extent that any law or Executive order specifically

limits the exercise of such authority to persons at the Secretarial level of a Military Department, such authority shall be exercised by the appropriate Under Secretary or Assistant Secretary of Defense.

These delegations of authority are effective immediately.

SORT: 1025.5

DOCI: DODI 1025.5

DATE: 19950213

TITL: DODI 1025.5 National Security Education Program (NSEP) Grants to Institutions of Higher Education, February 13, 1995, ASD(S&R)

References: (a) DoD 5025.1-M, "DoD Directives System Procedures," August, 1994, authorized by DoD Directive 5025.1, June 24, 1994
(b) Sections 1901-1910 of title 50, United States Code (David L. Boren National Security Education Act of 1991, December 4, 1991, as amended)
(c) DoD Directive 1025.2, "National Security Education Program," January 13, 1993
(d) Section 1141 of title 20, United States Code (The Higher Education Act of 1965)
(e) DoD Instruction 1025.3, "Administrator, National Security Education Program," January 19, 1993

A. PURPOSE

This Instruction, following DoD Directives procedures in reference (a), implements policy, assigns responsibilities, and prescribes procedures under references (b) and (c) by which institutions of higher education apply for, and are awarded, grants under the NSEP.

B. APPLICABILITY

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

C. DEFINITIONS

Terms used in this Instruction are defined in enclosure 1.

D. POLICY

It is DoD policy that:

1. Grants shall be awarded to accredited public or private U.S. institutions of higher education (reference (d)) to enable these institutions to establish, operate or improve programs in foreign languages, area studies, and other international fields that are critical areas of those disciplines (as determined under Section 1902(a)(1)(c) of reference (b)). Other U.S. or foreign organizations, associations, and agencies may be included in proposals but may not be direct recipients of a grant.

2. Program participation shall be restricted solely to those institutions of higher education, associations, organizations, and other entities that do not discriminate against applicants, students, and employees on the basis of race, religion, sex, color, disability that is not disqualifying, age, or national or ethnic origin and do not bar on campus military recruiting.

E. RESPONSIBILITIES

The Assistant Secretary of Defense for Strategy and Requirements (ASD(S&R)), directly or by assignment to the Director of the NSEP (reference (e)), shall:

1. Make available competitive grants to U.S. institutions of higher education to enable these institutions to establish, operate, or improve programs in foreign languages, area studies, and other critical international fields,

2. Administer, or designate an appropriate administrative agent to administer, the grants program.

3. Ensure that institutions of higher education or organizations competing for grants shall:

a. Adhere to the guidance for submitting preliminary proposals provided in this Instruction and in the application issued for each annual competition.

b. If invited to submit a full proposal, adhere to the guidance for submitting a full proposal provided in this Instruction and in the application issued for each annual competition.

4. Approve final grant recommendations of the independent review panels.

5. Ensure that institutions of higher education or organizations that are recipients of grants shall:

a. Complete the project and fulfill the conditions contained in the proposal upon which their award was based.

b. Advise the Assistant Secretary of Defense for Strategy and Requirements (ASD(S&R)) if conditions develop which would prevent the award recipient from carrying out the program specified in their proposal.

6. Ensure that the Administrative Agent, or other entity designated by the Secretary of Defense or ASD(S&R) to administer the grants program, shall, consistent with section D.1-2, above, administer the program on behalf of the Secretary.

F. PROCEDURES

1. The National Security Education Program Office (NSEPO) will announce annually a competition for NSEP Institutional Grants beginning in the spring and ending in the fall.

2. United States institutions of higher education qualified to compete for NSEP grants as defined in reference (b), section 1908(3) and reference (d), can obtain application forms and information by:

a. Writing to:

National Security Education Program
Rosslyn P.O. Box 20010
1101 Wilson Boulevard, Suite 1210
Arlington, VA 22209

b. Sending a facsimile request to: 703-696-5667 or by

c. Sending an Internet message to: nsep@policy1.policy.osd.mil

3. Grants to institutions are designed to:

a. Complement NSEP scholarship and fellowship programs by encouraging the development of programs and curricula that:

(1) If prove the quality and infrastructure of international educational opportunities.

(2) Address issues of national capacity.

(3) Define innovative approaches to issues not addressed by NSEP scholarship and fellowship programs.

b. Enhance institutional capacity and increase the number of faculty who can educate U.S. citizens to:

(1) Understand less commonly taught languages and cultures and become involved in global issues.

(2) Build a critical base of future leaders in the marketplace and in Government service who have cultivated international relationships and worked and studied alongside foreign experts.

(3) Develop a cadre of professionals with substantial knowledge of language and culture who can use this ability to make sound decisions and deal effectively with global issues in their professions.

4. Grants will be awarded for 1 or 2 year periods. Any funding beyond 2 years will be based on an evaluation of the project and an assessment of its progress in meeting NSEP objectives (as specified in reference (b)) and will require reapplication through the established competition procedures.

5. Between Sand 25 awards of $25,000 to $250,000 per year for up to 2 years may be made in each competition. Awards will not exceed $250,000 per year. Within the foregoing limits these are estimates and do not bind the NSEP to a specific number of grants or specific grant amounts.

6. Only U.S. citizens and U.S. institutions of higher education may receive NSEP funding as stipulated in reference (b). Student scholarships or fellowships funded through the NSEP institutional grants program shall only be awarded to U.S. citizens; non-U.S. citizens on exchange programs are not eligible for funds under the NSEP.

7. Only those requirements that govern all Federal grants shall be reflected in NSEP grant awards.

8. The NSEP U.S. Institutional Grants Program has a two-stage submission and review process: a preliminary stage and a final stage. To qualify for funding consideration, all applicants must submit a Preliminary Proposal (application).

9. Preliminary Proposals shall be submitted in accordance with submission procedures summarized in this paragraph and detailed in the grants application available from the NSEPO (section F.2 above).

a. An ORIGINAL AND SEVEN COPIES of the proposal must be submitted by the annually announced deadline to:

Acquisition Directorate
ATTN: Mr. Robert Lavelle (R-2)
Defense Supply Service-Washington
5200 Army Pentagon
Washington, DC 20310-5200

b. The burden of timely receipt is on the applicant. PROPOSALS MAY NOT BE SENT BY FACSIMILE.

c. A completed Grant Application Cover Sheet (enclosure 2) must cover each proposal.

d. The narrative, of no more than five pages, must be DOUBLE-SPACED and NUMBERED. It must describe a problem or need, offer a strategy to solve the problem or meet the need, and explain how the approach serves NSEP objectives. One or two additional pages of background material on the institution(s) involved in the proposal may be included separate from the five page narrative.

e. The applicant should use the Proposal Budget Estimate Worksheet (enclosure 3) to delineate proposal costs for either one or two year funding.

f. The NSEPO will mail confirmations with a Proposal Reference Number within two weeks of receipt of the proposal.

10. An independent review process will be coordinated by the NSEPO for a period of between 45 and 60 days from the date that the preliminary

proposals are due. Applicants will be notified by mail of the results of the preliminary review. A summary of readers' comments will be available from NSEPO upon request. Those institutions whose proposals were determined to be eligible to submit final proposals will be notified in writing and by telephone.

11. Final Proposals shall be submitted in accordance with submission procedures for Preliminary Proposals summarized above (except as amended below) and detailed in the grants application available from the NSEPO (see section F.2 above).

a. Final proposals will be due no earlier than 45 days and no later than 60 days from the date that the final competition commences. The exact due date will be specified each year in the grant application.

b. In block 8 of the Proposal Cover Sheet, an abstract must be included giving a concise statement of the problem, proposed activities, and the program's potential for contributing to the national capacity.

c. The proposal narrative, of between 15 and 25 DOUBLE-SPACED pages, should discuss how the proposal addresses the NSEP criteria specified in section F.3 above and described in detail in the application form.

d. Following the Proposal Budget Estimate Worksheet (enclosure 3) a narrative budget statement should be attached explaining:

(1) The basis used to estimate professional personnel, consultants', travel, indirect costs and any other costs that may appear unusual.

(2) How major cost items relate to the proposed project activities.

(3) Costs of the project's evaluation component.

e. Any assurances and certificates required by the Federal Government should be enclosed.

12. Proposals will be evaluated by merit review panels of primarily faculty and administrators from higher education, although some reviewers might be from the non-academic research and business communities. Consistent with judgments based on merit, efforts will be made to ensure balance (geographical, ethnic, gender, institutional type and subject matter) across the entire competition.

13. Proposals will be evaluated according to the following selection criteria which are summarized in this paragraph and described in detail in the application:

a. Significance of the problem. The proposal must address issues of national capacity and identify needs, gaps and/or shortfalls in the national capacity. The proposal should explain why the gaps exist and how the proposal will fill the need. It must show familiarity with the state of the field in the proposal area.

b. Response to the problem. The proposal must present a credible, appropriate and original response to the needs and gaps identified.

c. Prospects for wider impact. The proposal must address national capacity and clearly show how it will have impact beyond a specific campus. The impact on students and diversity will be considered.

d. Cost-effectiveness. Proposals will be evaluated on the basis of "educational value for the dollar." The feasibility of the budget plan, the likelihood of continued support for the program for 3 to 5 years after the NSEP grant period, and the extent of non-NSEP funding to support the program will be considered.

e. Capacity and commitment of the applicant. The proposal must demonstrate a clear commitment to the project by the institution including a willingness to bear a reasonable and increasing share (over 3 to 5 years) of the direct and indirect costs of the project.

f. Evaluation plans. The proposal must have a clearly defined approach to measure the short, intermediate and long-term its impact on language competency, foreign cultural competency, and the value of study abroad experiences (where appropriate) and the flexibility to make

modifications to increase impact.

G. INFORMATION REQUIREMENTS

Information collection requirements imposed by this issuance are licensed under Office of Management and Budget (OMB) Control Number 0704-0366.

H. EFFECTIVE DATE

This Instruction is effective immediately.

Edward L. Warner, III
Assistant Secretary of Defense
for Strategy and Requirements

Enclosures

1. Definitions
2. Proposal Cover Sheet
3. Proposal Budget Estimate Worksheet
4. Expanded Definition: Institutions of Higher Education

1. Administrative Agent. An organization, association, college, or university given authority by the Secretary of Defense to administer and monitor the grants program. Administrative agents must be private, not-for-profit organizations, associations, or institutions.

2. Aggregate. The sum of the days of award assistance granted to a scholarship or fellowship recipient.

3. Award. Any amount of financial assistance given to an institution of higher education as a grant under the NSEP.

4. Critical Area. A language, country, geographic area or region, other than one traditionally focussed upon by U.S. institutions of higher education, and where limited capacity for study currently exists. This definition excludes countries of Western Europe, Canada, Australia and New Zealand.

5. Federal Government. Organizations and Agencies that comprise the executive, legislative, and judicial branches of the U.S. Government.

6. Field of Education. Activities where teaching or research is a primary responsibility and is conducted in institutions of primary, secondary, or postsecondary education, or where such activities take place in a recognized organized educational or instructional environment.

7. Grant. A financial award made to an institution of higher education under this program based on the relative merit of a proposal submitted by that institution to the NSEP office during specified periods of competition for such awards.

8. Indirect Costs. These costs, also called "overhead" are understood to be negotiated by institutions of higher education with the Federal Government. NSEP institutional grants are assumed to be for training programs, thus, indirect costs associated with training programs should be used as a benchmark for determining appropriate overhead rates.

9. Institution of Higher Education. A U.S.-accredited community college, or an accredited college or university with postsecondary degree-granting authority, as defined in section 1201(a) of the Higher Education Act of 1965 (reference (d)).

10. National Capacity. The concept of national capacity refers to the goal of the NSEP to provide opportunities to more U.S. students and institutions to improve their capabilities in understanding and adapting to other languages and cultures.

11. National Security. Economics, foreign affairs, and defense generally characterize the scope of national security.

12. National Security Education Board. A 13-member board established by the Secretary under the provisions of Section 803 of Public Law 102-183 (1991) (reference (b)) with responsibilities as specified therein.

13. National Security Education Program Group of Advisors. A body of senior education, business, and private sector representatives who provide advice to the National Security Education Board and to the Program Office, and provide for a communication exchange between higher education and the Federal Government.

14. National Security Education Program Office (NSEPO). The office established to administer the NSEP.

15. National Security Education Program Director. This official is the Administrator of the NSEP (reference (e)).

<<|IMAGE DODI0001.gif|>>

<<|IMAGE DODI0002.gif|>>

<<|IMAGE DODI0003.gif|>>

DEFINITION OF INSTITUTION OF HIGHER EDUCATION

The National Security Education Act of 1991 (reference (b)) stipulates this as the definition to be applied in the conduct of the program. The following definition is quoted from reference (d).

"(a) The term `institution of higher education means an educational institution in any State which (1) admits as regular students only persons having a certificate of graduation from a school providing secondary education, or the recognized equivalent of such a certificate, (2) is legally authorized within such State to provide a program of education beyond secondary education, (3) provides an educational program for which it awards a bachelor's degree or provides not less than a two-year program which is acceptable for full credit toward such a degree, (4) is a public or other nonprofit institution, and (5) is accredited by a nationally recognized accrediting agency or association, or if not so accredited, is an institution that has been granted preaccreditation status by such an agency or association within a reasonable time. Such term also includes any school which provides not less than a one-year program of training to prepare students for gainful employment in a recognized occupation and which meets the provisions of clauses (1), (2), (4), and (5). Such term also includes a public or nonprofit educational institution in any State which, in lieu of the requirement in clause (1), admits as regular students persons who are beyond the age of compulsory school attendance in the State in which the institution is located. For purposes of this subsection, the Secretary shall publish a list of nationally recognized accrediting agencies or associations which he determines, pursuant to subpart 3 of part G, to be reliable authority as to the

Index

SORT: 3300.2

DOCI: DODI 3300.2

DATE: 19940207

TITL: DODI 3300.2 Combined **Intelligence** Publishing Service (CIPS), February 7, 1994, ASD(C3I)

A. PURPOSE

This Instruction establishes the CIPS within the Department of Defense to assure that **intelligence** printing, publishing, and dissemination (IPPD) is accomplished effectively and efficiently in a manner conducive to national security and consistent with the authorities and duties of the Secretary of Defense under reference (a) and with references (b) and (c). Also, designates the Director, CIPS, as the DoD Executive Agent for IPPD.

B. APPLICABILITY AND SCOPE

This Instruction applies to:

1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as the "the DoD Components").

2. All IPPD tasks performed by non-**intelligence** activities.

C. DEFINITIONS

1. **Intelligence**. General military **intelligence**, scientific and technical **intelligence**, human **intelligence**, indications and warning,

current **intelligence**, estimates and analysis, communications security, information systems security, signals **intelligence**, training, and security and administration of **intelligence** operations, produced and disseminated by any method or media, electronic, or mechanical. Recipients range from DoD and national-level planners and decision makers to operational field commanders.

2. **Intelligence** Activities. All DoD **intelligence** printing, publishing, and dissemination activities. This includes **intelligence** collection, production, and dissemination activities not directly assigned to **intelligence** over which **intelligence** has been assigned responsibility for printing, publishing, and dissemination.

3. **Intelligence** Printing, Publishing, and Dissemination (IPPD). The technical processes of composition, photography, assembly, printing, duplicating, reproduction, binding, finishing and dissemination of publications, optical digital technology, and microform or electronic publishing media in support of **intelligence**.

D. POLICY

It is DoD policy to assure that a single organization, the CIPS, is responsible for the effective and efficient performance of **intelligence** printing, publishing, and dissemination.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence** shall oversee and review the implementation of this Instruction.

2. The Heads of the DoD Components shall ensure that their organizations support the CIPS in accordance with procedures and guidance established by this Instruction.

F. PROCEDURES

1. The Assistant Secretary of Defense for Command, Control, Communications, and **Intelligence**, in accordance with 10 U.S.C. and DoD Directives 5137.1 and 5330.3 (references (a) through (c)), shall:

a. Have principal OSD staff responsibility for the policy governing activities of the CIPS and provide this policy guidance regarding the operation and management of IPPD in the Department of Defense through an Executive Steering Committee.

b. Establish and chair the Executive Steering Committee composed of principals from major DoD **intelligence** activities.

c. Represent DoD **intelligence** IPPD matters to the DoD Printing and Duplicating Services Oversights Group, the Defense Printing Service, the Congressional Joint Committee on Printing, the Government Printing Office, the Office of Management and Budget, and other Government Agencies.

d. Assure maximum complementary support between DoD **intelligence** printing and publishing programs and comparable activities within the National Foreign **Intelligence** Program (NFIP), Information Systems Security Programs (ISSP), and the Consolidated Cryptologic Program (CCP).

2. The Director, Defense **Intelligence** Agency, is assigned responsibility for management of the CIPS and, in accordance with references (a) through (c), shall:

a. Appoint a Director, CIPS, to manage and operate the CIPS and all assigned responsibilities and who shall be under the authority, direction, and control of the Director, Defense **Intelligence** Agency (DIA).

b. Provide administrative support to the CIPS, to include personnel, budget execution, and contracting services.

c. Ensure that the Director, CIPS, in accordance with policy, procedures, and guidance approved by the ASD(C3I), shall:

(1) Organize, direct, and manage the CIPS and its assigned resources, and administer, supervise, and control all assigned programs, services, equipment, systems, and functions.

(2) Assure that IPPD is achieved in an effective and efficient manner conducive to national security, consistent with the authorities and duties of the Secretary of Defense under 10 U.S.C. (reference (a)).

(3) Evaluate the performance of IPPD components of the DoD and make recommendations to the ASD(C3I) on program and policy guidance.

(4) In coordination with the appropriate DoD Components, support, conduct, and approve research and development activities, facility establishment, facility upgrade, equipment procurement, equipment disposition, and IPPD activities consistent with applicable law and DoD Directives.

(5) Coordinate and facilitate the development and selection of IPPD standards, future needs, and requirements reporting.

(6) Convene joint working groups and/or committees as required.

(7) Advise the ASD(C3I) on **intelligence** printing and publishing standards, future needs, and requirements.

(8) Perform such other functions related to DoD IPPD as the ASD(C3I) may direct.

3. The Directors of the National Security Agency and the Defense **Intelligence** Agency, in accordance with 10 U.S.C. and DoD Directives 5137.1 and 5330.3 (references (a) through (c)), shall be advisors to the CIPS on the planning, development, implementation,

and evaluation of DoD IPPD within the ISSP/CCP and the General Defense **Intelligence** Program, respectively, and other related NFIP programs for which they are the functional manager.

4. The Heads of the DoD Components, in accordance with references (a) through (c), shall:

a. Provide, in accordance with established procedures and guidance, necessary staffing and resources to enable CIPS to accomplish its mission.

b. Assure that the Combined **Intelligence** Publishing Service Advisory Council (CIPSC) shall be composed of senior managers nominated by DIA, the National Security Agency, the Defense Mapping Agency, the Service **intelligence** components, the Unified Commands and other designated **intelligence** activities within the Department of Defense. The representatives shall attend periodic scheduled meetings as well as ad hoc meetings as required by the Director, CIPS.

c. Appoint a representative to the CIPSC who will act to carry out the responsibilities within member organizations on all IPPD activities required to implement the approved programs.

d. Assure that the Deputy Director, CIPS shall be nominated and funded by the **intelligence** activities (non-DIA) of the DoD **Intelligence** Community and will rotate among those activities every three years.

e. Assure that the CIPS Council shall:

(1) Be chaired by the Director, CIPS.

(2) Assist Director, CIPS in the development of IPPD procedures and guidance for the more effective and efficient management of IPPD activities.

(3) Support the Director, CIPS, and provide necessary

information and assistance in determining requirements, arranging for and executing inter-component support agreements, and enabling the CIPS to carry out day-to-day operations in an effective and efficient manner.

(4) Convene joint working groups and/or committees as required.

G. EFFECTIVE DATE

This instruction is effective immediately.

Emmett Paige, Jr.
Assistant Secretary of Defense
(Command, Control, Communications
and **Intelligence**)

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English

Let's confirm you are human

Complete the security check before continuing. This step verifies that you are not a bot, which helps to protect your account and prevent spam.

Begin >

English